NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**NETWORK CENTRIC WARFARE:
A REALISTIC DEFENSE ALTERNATIVE FOR
SMALLER NATIONS?**

by

Jan Berglund

June, 2004

Thesis Co-Advisors: John Arquilla
Gordon H. McCormick

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Network Centric Warfare: a Realistic Defense Alternative for Smaller Nations			**5. FUNDING NUMBERS**
6. AUTHOR Berglund, Jan			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This thesis establishes an analytical framework for identifying and discussing strategic factors considered important when implementing NCW as a new warfighting concept for the information age. Although the findings have a broad application, focus has been on a Norwegian NCW implementation. A key question is if the emerging NCW concept is a feasible defense alternative for smaller nations.

Central to the study are factors found in the strategic environment, such as Norway's strategic freedom of maneuver, affiliation with NATO, the impact of national interests, economic and technological assumptions, and the cultural premises that underlie the power of information. The changing features in the nature of conflict and in future potential opponents will also influence NCW mission challenges, opportunities and constraints. A particularly important mission challenge is the neglected military view of low-intensity conflicts as "worthy" military missions as well as the sociological impact on networked actors and opponents, as conditioned by new trends in the information age.

A key finding is that NCW, which also takes into consideration the impact of other strategic factors discussed in this thesis, has the potential to rise to the many challenges and achieve many of the objectives currently "floating" in existing military transformation strategies.

14. SUBJECT TERMS Network Centric Warfare, Transformation, Strategy, Low-intensity conflicts, Military Doctrine & Organization			**15. NUMBER OF PAGES** 160
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

NETWORK CENTRIC WARFARE: A REALISTIC DEFENSE ALTERNATIVE FOR SMALLER NATIONS?

Jan Berglund
Commander, Royal Norwegian Navy
B.S., Royal Norwegian Naval Academy, 1992

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
June 2004

Author: Jan Berglund

Approved by:
John Arquilla

Gordon McCormick
Thesis Advisors

Gordon McCormick
Chairman, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis establishes an analytical framework for identifying and discussing strategic factors considered important when implementing NCW as a new warfighting concept for the information age. Although the findings have a broad application, focus has been on a Norwegian NCW implementation. A key question is if the emerging NCW concept is a feasible defense alternative for smaller nations.

Central to the study are factors found in the strategic environment, such as Norway's strategic freedom of maneuver, affiliation with NATO, the impact of national interests, economic and technological assumptions, and the cultural premises that underlie the power of information. The changing features in the nature of conflict and in future potential opponents will also influence NCW mission challenges, opportunities and constraints. A particularly important mission challenge is the neglected military view of low-intensity conflicts as "worthy" military missions as well as the sociological impact on networked actors and opponents, as conditioned by new trends in the information age.

A key finding is that NCW, which also takes into consideration the impact of other strategic factors discussed in this thesis, has the potential to rise to the many challenges and achieve many of the objectives currently "floating" in existing military transformation strategies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis is the result of a long thought process starting in the late nineties, about how Norway could meet the expenses and difficult challenges of adapting its military to the information age. Although I recognized the promising properties of the new visions and warfighting concepts in military affairs, I have also thought that there was a certain lack of application of a strategic perspective in the same. My academic background from the Naval Academy and the Norwegian Defense College, along with my job experiences as an officer in the Norwegian Naval Special Forces, and also as a staff officer at the former Defense Command North-Norway, has contributed greatly to the way I perceive the new warfighting concepts and the future defense challenges facing the Norwegian military.

Most influential in my thesis research, however, have been my studies in Monterey at the Naval Postgraduate School, Department of Defense Analysis. The quality of faculty and staff members and the variety of subject matter in the course offerings in the Special Operations Curriculum have been invaluable in encouraging the approach to and thought about military problems from a strategic perspective. Also, I have been able to draw on the plentiful resources found in my immediate surroundings. A special thanks to my thesis advisors Professor John Arquilla and Professor Gordon H. McCormick for assisting in shaping my concepts and methodology and for constructive guidance in the writing process.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis identifies and discusses several strategic factors considered important when implementing NCW as a new warfighting concept for the information age. Although the findings have a broad application, my focus has been on NCW implementation in the NATO Alliance's small countries, and in Norway in particular. Of particular interest are factors found in the strategic environment. For Norway's case, as a non-EU member state, strategic freedom of maneuver is determined by the power triangle between the U.S., the EU and Russia. The impact of this power triangle, and in particular the proximity of Russia, suggests that Norway must develop a broader range of NCW capabilities compared to other small nations. Furthermore, Norway's economic strength and technological environment imply a sound foundation for an NCW implementation if there is a willingness to prioritize the required strategic, doctrinal and organizational elements in an implementation strategy. As a small, high-tech oriented and transparent nation, Norway could particularly benefit from a broad interagency approach to the NCW concept. Other factors such as a cultural resistance to embracing the significance of soft power such as IO and public diplomacy as tools in information-age conflicts must be overcome in order to fully exploit the anticipated benefits of NCW.

Characteristics of the ongoing changes in the nature of conflict will also influence a NCW implementation strategy. New doctrinal and organizational principles such as swarming and the increased significance of trust in modern societies, should be further investigated to enhance future command and control arrangements and other NCW capabilities. In addition, the development of comprehensive mission capabilities must be ensured. Other mission challenges and constraints that need to be considered are the risk of shortcutting strategies and an underestimation of nontraditional missions found in low-intensity conflicts, caused by an exaggerated belief in Western militaries current supremacy, new warfighting capabilities and in the concept of information superiority.

Another important mission challenge discussed is the neglected military view of low-intensity conflicts as less "worthy" military missions. Obviously there is reluctance in the military to embrace these new and changing missions such as peace support- and

humanitarian operations even if they have political, economic and social significance. Noticeably, there is a need to transform both our understanding of low-intensity conflicts and our war fighting capabilities to meet the information revolution. Applying the revolution in military affairs only to the conventional, mid- and high intensity levels of war will not contribute to solving the difficult and complex problems connected with low-intensity conflicts. The scale of conflict is not a continuous line with just a higher intensity of the same problem. High-and low-intensity conflicts are in fact inverse problems with vastly different origins and threat assessments. They require different strategies, tactics and form of organization in order to be solved. Recognizing this diversity in future NCW development implies that both capabilities are needed, and that the types of forces employed in each case are not necessarily compatible or interchangeable.

The sociological impact of new trends in the information age, such as the emergence of smart mobs, should be further researched and exploited in future doctrines for conducting low-intensity conflict. Although, smart-mob behavior is based on developments in information technology, particularly in wireless networks and wearable mobile devices, it is the anticipated changes in social behavior and its impact on future networked actors and opponents that are significant. The benefits of smart-mob behavior for these actors can be substantial, but at the same time severe constraints apply. The NCW implications of smart-mob behavior are many, but two stand out. First and foremost are the requirements of network centric forces to understand and predict the consequences of this type of behavior by opponents or other actors in low-intensity conflicts. Second is the opportunity to develop new doctrinal concepts for homeland defense structures as well. In Norway's case, an example could be to introduce NCW capabilities in the home guard. The deterrent and operational impact of such a force could be considerable if the force truly were able to operate autonomously with the advantages of new information technology, combined with detailed local knowledge in the cities and in rural territories.

Finally, NCW has the potential to substantiate and unite the many challenges and objectives currently "floating" in existing transformation strategies. The continuous

process of a transformation strategy needs direction. The developments of Norwegian NCW, which also take into consideration the impact of strategic factors as discussed in this thesis, offers the prospect of shaping the transformation process and creating a comparative strategic advantage. In its present form, NCW might not be the proper concept or even the right term to use for how Norway should contribute militarily in future conflicts. But current theory, experiences and related experimental doctrines have come far enough for us to outline a more tangible and comprehensive concept. In this regard, the Norwegian adapted term *Network-Based Defense* or perhaps *Net-centric Defense* may be more appropriate than the term *Network Centric Warfare,* because it encompasses all levels of conflict and meets the requirements of net-centric activities: cooperation or integration across services; joint units; and inter-agency and multinational entities. Thus, NCW may be just the warfighting concept used during times of crisis or conflict to achieve or promote specific objectives over specific adversaries. Consequently, if net-centric operations are seen as the cornerstone of future warfighting concepts, it should indeed be pursued on a broader level in a comprehensive Norwegian transformation strategy. By doing so, *Network Centric Defense* has the potential to become a feasible and "holistic" defense alternative. To get there, we must rethink and broaden the whole business of military affairs, take some calculated risks towards an uncertain future, and emphasize the development of unconventional doctrinal and organizational concepts in a network-centric direction.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. DEFINING THE CONTEXT OF NETWORK CENTRIC WARFARE

Network centric warfare (NCW) is emerging as a future warfighting concept in the U.S., NATO and many other Western countries. NCW may be defined as "an information-superiority enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization."[1]

NCW arose out of the contemporary Revolution in Military Affairs (RMA). Arguably, this revolution represents a major discontinuity in military affairs due to the effects and prospects of new technology and in particular developments in information technology.[2] The United States is in front of doctrinal and technological developments, while its allies are adapting and developing their own NCW concepts based on their countries' individual premises and the Alliance's demands. This process is not simple and there are frictions and numerous problems associated with it based on the cultural, doctrinal, technological, and economic diversity within the Alliance.

At one end of the scale we find U.S. forces' long-term goals as they are envisioned in *Joint Vision* 2020: to form a joint force capable of full spectrum dominance on the battlefield.[3] Full spectrum dominance is an ambitious national goal in any type and level of conflict, and it is certainly not within reach of most other countries. For the new and less resource-rich NATO members in the Baltic and in Eastern Europe, who represent the other end of the scale, the goal is basically to develop an armed force that can fulfill fundamental national security needs and at the same time fit in with the Alliance's basic interoperability requirements. Other more established NATO members in Europe are also struggling to keep up with developments.

---

[1] David Alberts, John Garstka, and Frederick Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority,* (CCRP Publication Series, 1999), *2.*

[2] Several scholars dispute the assertion that a contemporary revolution in military affairs is taking place. However, most would agree that the current technological, doctrinal and organizational development has at least a potential to be called revolutionary by definition.

[3] Joint Chiefs of Staff, *Joint Vision 2020* (Washington: U.S. Government Printing Office, June 2000), 3.

It is within the context of the Information Age, the discontinuation of the Cold War's effect on the strategic environment and on the nature of war, and the subsequent military transformation process that NATO and most other Western countries have deemed necessary, that the NCW concept is evolving. How the latter is conducted is of particular importance since it is a direct and interrelated link between the two. According to Admiral E. P. Giambastiani, the current Supreme Allied Commander Transformation, transformation applies to the military by:

> …bringing changes to doctrine, organization, capabilities, training, education and logistics. It is not just about new weapon systems and improving capabilities. It is understood that Transformation is a process and a mind-set. It is an iterative, ongoing process that seeks to adapt and master unexpected challenges in a very dynamic environment. It is about managing the future in a joint and combined way.[4]

In this view, transformation is an optimized strategy that continuously tries to fit the defense structure to current and future security challenges. Thus, transformation differs from modernization because it aims not only at improving existing defense concepts, doctrines, organizations, logistics and tactics, but to change them in accordance with a dynamic environment. It is not only about doing things right anymore, but rather about doing the right things.[5] Critics, however, argue that the transformation process itself is on the wrong track or that it overshadows the strategic context in which NCW must be regarded.[6] Some of the allegations are that military transformation has a too narrow focus and that NCW is seen mainly as a technological and information superiority enabled concept at the operational and tactical level. It does not sufficiently take into

---

[4] Edmund P. Giambastiani. "What is Transformation?" Allied Command Transformation Web Page. Not dated. http://www.act.nato.int/transformation/transformation.html (Accessed 12 May 2004).

[5] Jørgen Berggrav, "Militær Transformasjon, en nødvendighet for å møte fremtiden?" The Norwegian Atlantic Committee, *Kortinfo – 3 2003,* August 2003 [journal online]; http://www.atlanterhavskomiteen.no/publikasjoner/andre/kortinfo/2003/3-2003.htm . (Accessed 26 January 2004).

[6] For critics of the military transformation process, see; Senior Analyst Marcus Corbin in *Rumsfeld's War Leaves Iraq in Pieces* Center for Defense Information April 14, 2004. http://www.cdi.org/mrp/corbin-newsday-041403-pr.cfm . Military historian Fredrick Kagan in *The Art of War* http://host45.ipowerweb.com/~newcrite/cgi-bin/printpage.php , and in *War and Aftermath* available at *http://www.policyreview.org/aug03/kagan.html* , and an early critique of the process by Professor Thomas Barnett, U.S. Naval War College with Henry H. Gaffney in *A Critique of the National Defense Panel Report* . The CNA Corporation, April 1998. http://www.geocities.com/ResearchTriangle/Thinktank/6926/ndpzero.htm (Accessed April 14 2004)

account the transformation of war, including the emergence of low-intensity conflicts and new problems in the third world.

Simplified, current descriptions of the NCW concept are not fully taking into account the strategic or political factors that directly or indirectly will influence conceptual, doctrinal and organizational development. Moreover, although many of these strategic factors will be common for most NATO countries, some will be dependent on specific conditions applicable to the individual countries in the Alliance. Hence, these conditions need to be studied independently by each nation before the concept is implemented.

This thesis will investigate some of the strategic factors that will influence the NCW concept in Norway, one of the smaller countries in the Alliance. A U.S.-led NCW bandwagon might not be appropriate for Norway in all its facets, considering the differences in resources, political objectives, threats, social structure, culture and other strategic preconditions. Consequently, and even if many of the forthcoming challenges imposed by the information age will apply to both, Norway is perhaps better off choosing a somewhat different track for its NCW train.

A thesis question pertinent to the above is therefore: **How will factors such as the strategic environment, changes in the nature of war and characteristics of our potential adversaries imposed by the information age, affect the development of a Norwegian NCW concept?** Will the emerging NCW concept be characterized as fractioned chaos or is it a feasible, holistic defense alternative also for smaller nations.

B. THE NORWEGIAN APPROACH TO NCW

The process of developing a Norwegian NWC concept was officially initiated in 2000 as a result of a Norwegian Chief of Defense annual defense study. So far efforts have been concentrated on exploring the tenets of NCW, and the concept is identified as a long-term goal. However, transformation initiatives to make the force more net-centric are currently being undertaken. A few publications have been issued by the Norwegian Chief of Defense and the Norwegian Defense College. These documents give an introduction to NCW based on the U.S. developed theory and conceptual framework.

They are focused on theoretical command and control issues and the conceptual use of network centric warfare in military theory in general. In addition, Norway has established an innovative unit called the Norwegian Battlelab Experiment (NOBLE), whose main focus is to find operational solutions that may direct the Norwegian Armed Forces in a network centric and precision guided engagement direction.

Although the Norwegian efforts have had a fairly good start since 2000, military transformation in a NCW direction is extremely challenging. Assuming it will be as costly as some have predicted, a fully mature network centric force seems almost unattainable for a small country with less than 4.6 million inhabitants, even if Norwegian defense spending within the Alliance is exceeded only by the U.S. when counted per capita. For 2004, the Norwegian defense budget represents 1.87% of GNP and 4.87% of the state budget.[7] A Norwegian NCW concept is anticipated to demand immense investments within both the command and control structure and the force structure because of a profound gap in requirements between the old and the new warfighting concept.[8] The costs are related virtually to the entire military organization: the info-structure, sensor components, decision components, effect components, data fusion systems, systems to create necessary situation awareness and systems for self-organization.[9] Consequently Norway, like other countries in the Alliance, is facing huge investments in the implementation process. Much of the older material designed to stop an enemy within a static defense concept is in process of being phased out to free the necessary resources, but it is stated that Norway will have to live with its military heritage for years to come.[10]

Furthermore, politically important values such as the conscript system, the home guard concept, and widespread military support for civilian society are at risk. It is questionable if Norway has the need for, or is able to develop and purchase the necessary

---

[7] Norwegian MoD, "Defence budget." Alliance comparison derived from NATO statistics for the fiscal year 2003. http://www.dep.no/fd/norsk/publ/veiledninger/010011-120053/index-dok000-b-n-a.html . (accessed 19 Feb 2004).

[8] Norwegian Chief of Defence. "Konsept for nettverksbasert anvendelse av militærmakt" *Forsvarssjefens Militærfaglige Utredning 2003.* Oslo: 2003, 50.

[9] Ibid. , 46 - 50.

[10] Ibid. , 7.

technology and information structure to maintain these values. As a consequence, and without alternative implementation strategies, NCW may transform the Norwegian Armed Forced to a defense with certain "niche capacities." These capacities may be well fitted within NATO where they indeed are needed; but, there are serious domestic concerns that these forces will have a lesser deterrent effect compared to the force structure possessed during the Cold War, and that they will not be sufficient for Norway's need to sustain independent operations for homeland defense and crisis management on its own territory and adjacent waters.

Consequently, there is a need for Norway to have a closer look at its implementation strategy for NCW. So far the NCW approach has been evolutionary rather than revolutionary. One reason is the earlier mentioned heritage and lack of demonstrated NCW efficiency. The underlying NCW theory, necessary simulations, and real life battle experiences are so far too ambiguous and based on primarily U.S. experiences that may not be consistent with a smaller country's premises or security needs. From this perspective an evolutionary development might be the right approach. However, Norway should at least investigate different NCW approaches based on other historical examples and strategic factors that may be more suitable to Norwegian conditions. In light of rapid military technological, doctrinal and organizational developments, which constitute the three main areas of the emerging RMA, it is important to create a sense of urgency for the political and military leaders to make some consistent decisions for the way ahead. Nevertheless, possible consequences at all levels based on Norway's particular conditions should be analyzed before an implementation strategy is mapped out. This thesis aims to identify and evaluate some of the strategic factors that can contribute to developing an advantageous NCW implementation strategy in a Norwegian context.

C. METHODOLOGY

To establish a framework that may help to identify the strategic factors needed to create a comparative strategic advantage when implementing NCW, Michael Handel's

model for strategic planning have been adapted.[11] The model builds on the strategic thoughts of Carl von Clausewitz. Two of his analytical concepts are central. The first is about knowing the kind of war (s) that is forthcoming and the second is the well known trinity between the people, the military, and the government. If we add the material and technological environment that have characterized military innovation and developments the last century, and to which Clausewitz paid less attention , [12] the model could function as a starting point to identify factors that have strategic implications. These factors can in turn be analyzed in a network-centric context.

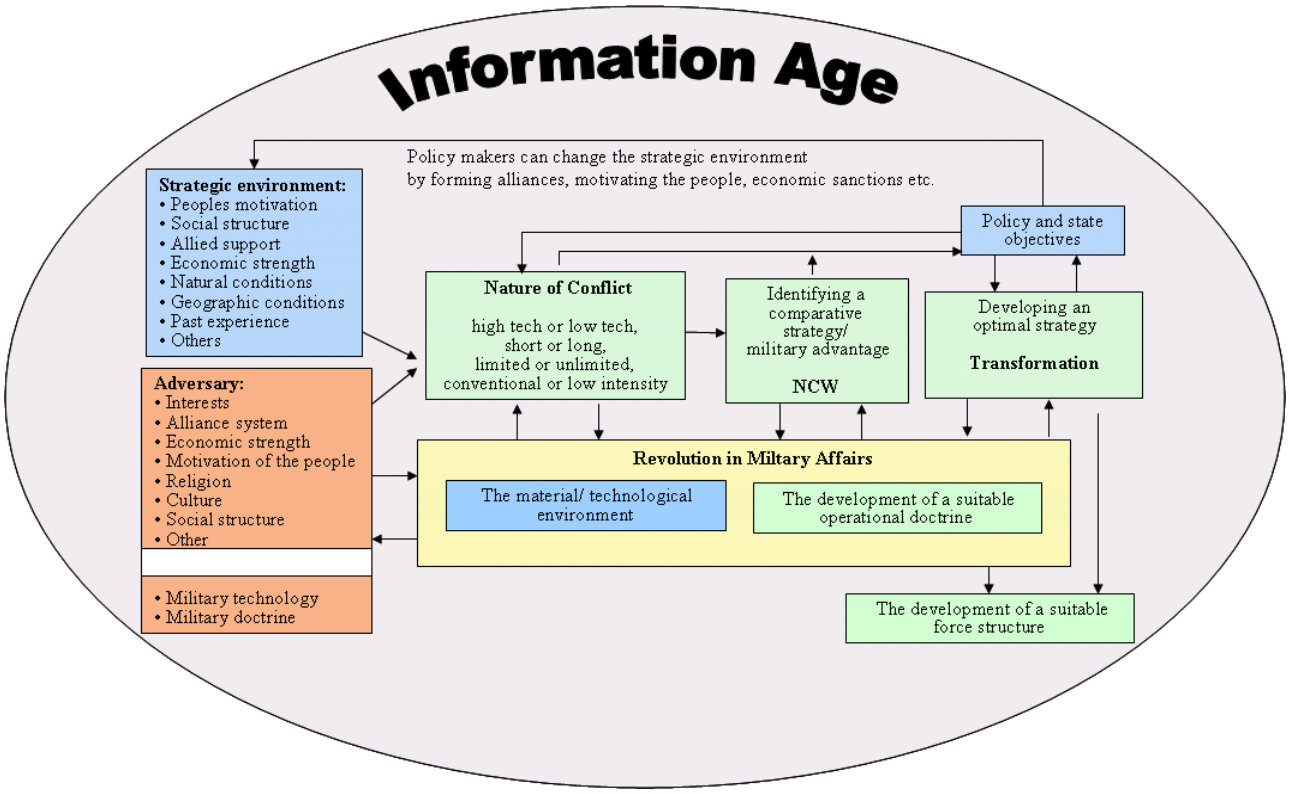

Figure 1. Identifying Strategic Factors (After Handel, 2001).

The analysis will begin in Chapter II by describing the NCW concept as it is presented by NCW proponents. Since NCW is part of a U.S. led RMA, U.S. literature has

[11] Michael Handel, *Masters of War* (London: Frank Cass Publishers, 2001), 101.

[12] Ibid. , 109.

been heavily relied on. What are the advantages of changing the military in a network centric direction? NCW's advent was in the first Gulf War where superior U.S technology and combat power clearly showed the impact of information technology on the conventional battlefield. Since then, the developments within military innovations, technology and organization have accelerated towards even more information dependent war fighting concepts based on precision guided munitions, real-time information dissemination, and on demand delivered logistics. The development has necessitated a shift from a platform-centric to a network-centric way of conducting warfare. Thus, *Network Centric Warfare* has been coined as the new term that describes how the military organize and fight in the Information Age. Chapter II presents a description of the NCW concept up to its present form. This background is necessary to understand the influence on the concept by the other factors depicted in Figure 1. It is assumed that Norway intends to follow the NCW path even if there exists, at least in theory, alternative security and defense policies that can lead to other warfighting concepts. This assumption also implies a limit to the scope of the thesis when addressing security and defense policies in the subsequent chapters.

The understanding of contemporary conflict is, among other things, determined by changes in the strategic environment and will be the theme for Chapter III. This chapter will discuss specific strategic factors that are believed should have a particularly important impact on the development of a Norwegian NCW concept. Some of the key issues are Norway's strategic freedom of maneuver, obligations and contributions within the Alliance; technological premises and other particulars of Norwegian social structure or culture that may or may not be well adapted to a NCW context. The latter premises have particular interest with respect to NCW, as an information superiority enabled concept because, as will be shown, Norway does not have a particularly well developed tradition of exploiting the soft power side of information. By soft power is meant the state's use of information as a recognized and important part of its power base, exercised through means such as public diplomacy, information operations or information warfare.

Chapter IV will discuss the impact of characteristics in the information age and the emerging RMA, in order to reach a deeper understanding of contemporary changes in the nature of war. This factor is central in Handel's model and an issue believed to have

been underestimated in the discussions of NCW so far. Perhaps the nature of conflict is a better term that also encompasses the new threats at the lowest end of the conflict scale. Although many of these changes have a universal application for most militaries emphasis will be on the consequences for Norway where deemed fit. Consequently, the implications these changes in the nature of conflict should have for future mission challenges, constraints and opportunities will be highlight. Particular attention will be paid to the features of low-intensity conflicts and the changing characteristics of potential adversaries imposed by the information age and the contemporary RMA.

In Chapter V there will be further exploration of certain aspects of low-intensity conflicts in light of the newest trends that are emerging in the information age. Recognizing that there is a need to combine both the understanding of low-intensity conflicts and the information revolution's impact on modern forms of war should direct the NCW concept to encompass not only conventional, mid- and high intensity level of conflicts, but also the often more complex problems that are connected with low-intensity conflicts. Thus, this chapter will look at some of the sociological aspects of the information revolution and its impact on key actors in low-intensity conflicts such as those with extremists, terrorists and insurgents.

The final chapter will summarize key findings in the previous chapters in a Norwegian military transformation context. The assumption is that an NCW analysis seen through these strategic lenses, should affect both the direction of the transformation process itself as well as the technological, doctrinal and organizational development of a Norwegian NCW concept.

II. UNDERSTANDING NETWORK CENTRIC WARFARE

A. CONCEPTUAL FRAMEWORK

Network Centric Warfare emerged in the nineties as a new war fighting concept. It was envisioned as a way to achieve U.S. forces' long-term goals as depicted in *Joint Vision* 2020: to form a joint force capable of full spectrum dominance on the battlefield. Full spectrum dominance should be achieved by the application of four key operational concepts[13]:

- Dominant maneuver
- Precision engagement
- Focused logistics
- Full dimensional protection

Furthermore, *Joint Vision* set the goal for "DoD to pursue information superiority in order that joint forces may possess superior knowledge and attain decision superiority during operations across the spectrum of conflict"[14].

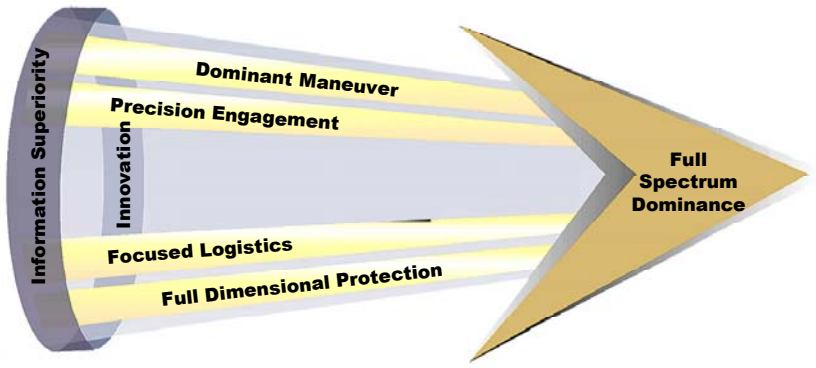

Figure 2. Full Spectrum Dominance Enabled (From *Joint Vision 2020)*

[13] Joint Chiefs of Staff, *Joint Vision 2020* , 3

[14] DoD, "Network Centric Warfare", Department of Defense Report to Congress (DoD 27 July 2001), 1-1. www.c3i.osd.mil/NCW/ (accessed 14 April 2004).

DoD envisions NCW to be a warfighting concept to achieve *Joint Vision* 2020 operational capabilities.[15] NCW allows " …the force access to a previously unreachable region of the information domain – the network region – that is broadly characterized by both increased information richness and information reach."[16] The information advantage is characterized as Information Superiority (IS). The significance of IS as an enabling factor is shown in Figure 2 as an enabling band across the operational capabilities. It is also inherent in DoD's definition of NCW, stated earlier in the Introduction. The correct interpretation of any given situation in an NWC concept is interdependent on three other essential capabilities as described by the Command and Control Research Program (CCRP).[17] In sum, the four minimum capabilities are:[18]

1. The ability to make sense of the situation;
2. The ability to work in a coalition environment including nonmilitary (interagency, international organizations and private industry, as well as contractor personnel) partners;
3. Possession of the appropriate means to respond; and
4. The ability to orchestrate the means to respond in a timely manner.

Throughout this thesis CCRP's conceptual framework and understanding of NCW will be used as a basis for discussions. The concept is depicted in the following figure which also encompasses the above mentioned capabilities. Furthermore, the model identifies the characteristics and attributes needed by NCW forces and their relationship to other entities.[19]

---

[15] DoD 27 July 2001, 2-4

[16] DoD 27 July 2001, 2-4

[17] CCRP is the driving force within the DoD and the U.S. Armed Forces for developing the NCW concept and has the mission of "…improving DoD's understanding of the national security implications of the Information Age"

[18] David Alberts and Richard Hayes, *Power to the Edge* (CCRP Publication Series, June 2003), 98.

[19] Alberts and Hayes, *Power to the Edge,* 99.

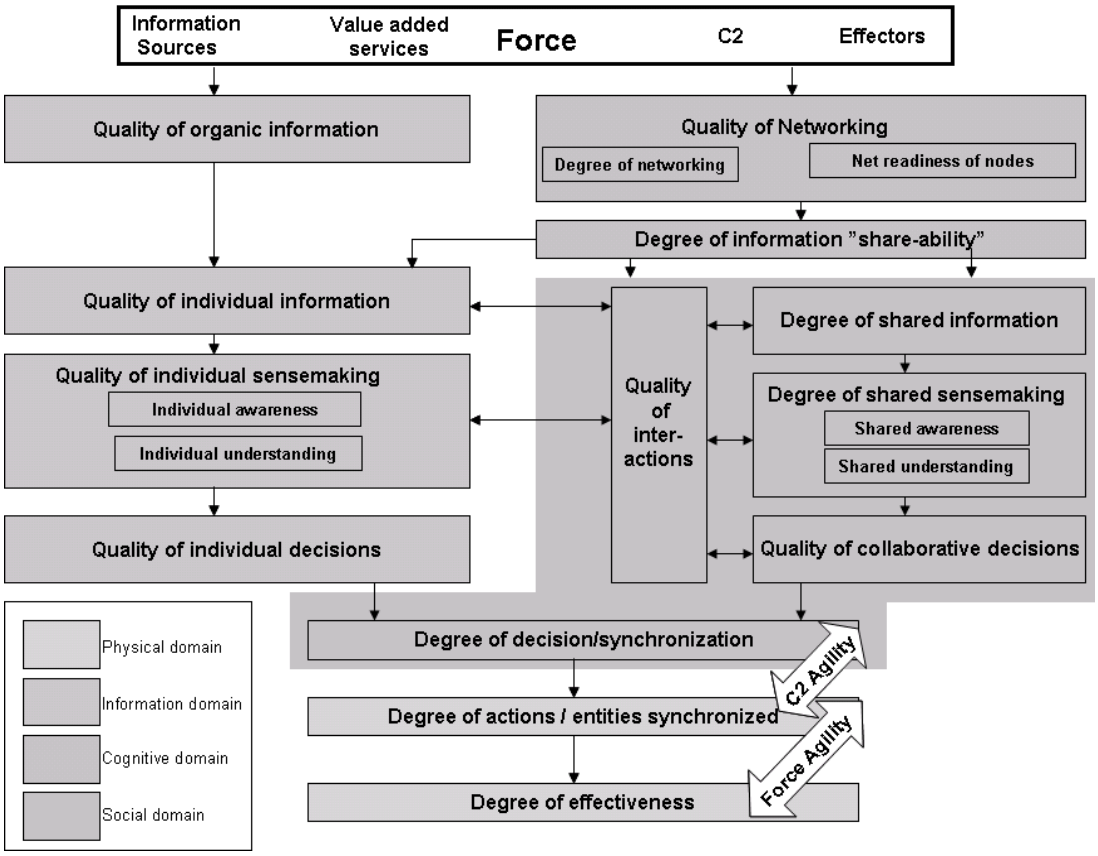

Figure 3. NCW Framework (From Albert and Hayes, 2003)

Alberts and Hayes explain the increased value of the NCW concept as follows: [20]

> The logic of the NCW value chain begins with the characteristics of force entities. These include effectors (all those able to create effects, not just weapons), information sources, value added services, and of course, command and control entities. Individual entities have access to organic capabilities including organic information sources. The degree to which force entities are networked will determine the quality of information that is available to various force entities and their ability to interact in the information domain. The level of interoperability achieved and the characteristics of command and control processes will determine the extent that information is shared, as well as the nature and quality of the interactions that occur between and among force entities. Taken together, these capabilities and organizational characteristics will determine the effectiveness of the force, its agility, and the degree to which decisions, plans, actions, and entities are synchronized.

In the following, the key elements in NCW, the concept of information superiority and the benefits of networking the force will be presented.

[20] Alberts and Hayes, *Power to the Edge,* 101.

B. THE CONCEPT OF INFORMATION SUPERIORITY

Information is power and information superiority is a key factor in NCW. IS affects all areas of modern warfare in the physical, information, cognitive and social domain. NCW impact on the four domains is depicted in shades of grey in Figure 3. The physical domain is where strike, protect and maneuver takes place, preferably in a joint perspective. The focus is primarily tactical, emphasizing hardware and battle space technology. This is also the area where NCW effects are easiest to predict and measure. Challenging military innovations within technology sectors such as sensors, stealth, speed, navigation (precision), and weapons systems are forthcoming, which in turn will contribute to establish IS. Nevertheless, most of the problematic aspects with the IS concept occur in the other domains that to a larger extent involve cultural and organizational changes. Changing people's mindset in the way they practice their business is inherently more difficult. Consequently, focusing on these domains will be important to achieve IS on a broad scale as envisioned in *Joint Vision* 2020.

Seeking out an information advantage to outperform an adversary is nothing new in military affairs. The principles of collecting information, processing it for intelligence and planning purposes and distributing it through the chain of command has been valued since the days of Sun Tzu. Furthermore, Clauswitz' term "the fog of war," and his notion about "friction" during the conduct of war, are closely connected to commanders' uncovered information needs. Presumably, commanders want to have all the relevant information they can get to analyze it, before they put men at risk. In addition, commanders must evaluate the validity of the provided information. Adversaries will most likely try to hide, disrupt or falsify information to conceal their own intentions.

All these activities take place in the informational, cognitive and social domain. The information domain is where information is collected, posted, pulled, displayed, processed and stored.[21] It is also the domain where command and control are communicated. The single most important information element traveling through this domain is perhaps the commander's intent, which also is based on the enemy's anticipated actions. The perception and understanding of the information takes place in

[21] Alberts and Hayes, *Power to the Edge,* 15.

the cognitive domain. Interpretation of the information is influenced by the values, frame of mind, presumptions and biases of the commander or the interpreter,[22] or, in other words, by the mindset of the warfighter and his aides. The response, or action, is reflected in the output of the interpretation, including the style and contents of such things as leadership, intent, doctrine, tactics and techniques. Lastly, but equally important to achieve an information advantage are the organizational aspects, the C2 processes and interactions between entities and individuals that take place in the social domain.

The difference in this notion of the term *information advantage* compared to the earlier one is that innovations in technology, and in particular information technology, have created possibilities for both quantitative and qualitative improvements in information processing. They have also created the conditions for network centric computing, which the explosive growth of the Internet and intranets has shown in the last decades. Some claim that these improvements are revolutionary in character because they will radically change how wars will be fought in the future. Hence, we are in the midst of a RMA.

The prospects of gathering and processing information to be able to lift Clausewitz's "fog of war," enabling commanders at all levels to have a transparent view of the battlefield, are alluring. Transparency of the battlefield will of course not be a constant or 100% condition but it will vary in time and space. Hence, the Joint Chiefs of Staff's definition of information superiority is, "The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same,"[23] must be interpreted accordingly. Information superiority is a condition only achieved when a force is able to exploit a superior information position compared to its adversary. The relationship is shown in the following figure.

[22] Alberts and Hayes, *Power to the Edge,* 15.

[23] Joint Publication 3-13. "Joint Doctrine for Information Operations" (Headquarters Department of the Army, 1998), GL-7.

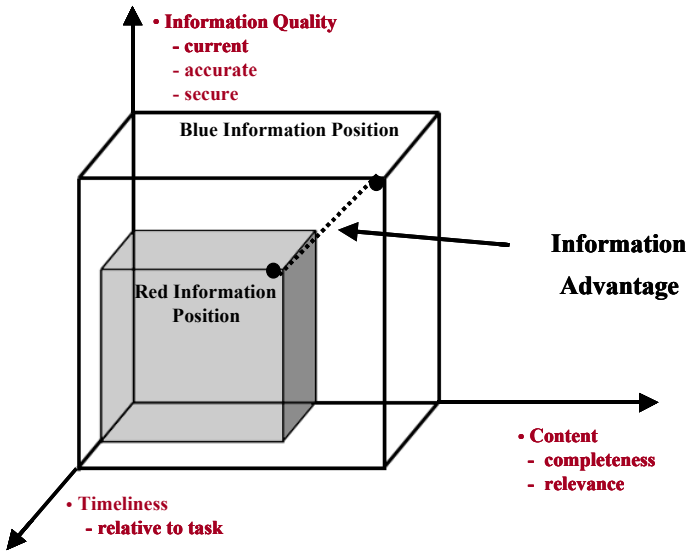

Figure 4. Information Advantage (From Alberts, Garstka and Stein, 1999)

According to J. Garstka at the Joint Staff Directorate for C4 Systems, some characteristics of this relative information advantage is that it can:

- Be persistent or it can be transitory.
- Exist in some areas of the battlespace but not others.
- Be measured in the context of a task or set of tasks.
- Be created by taking actions to reduce our information needs and/or increase the information needs of an adversary.
- Be achieved through the synergistic conduct of information operations, information assurance and information gain and exploitation".[24]

As Garstka suggests, Information Operations (IO) play a significant part in achieving IS. IO are "actions taken to affect adversary information and information systems while defending one's own information and information systems."[25] The desired effect of IO in the context of information superiority is "to drive one or more components of the competitor's information "volume" towards the origin. The desired effect of defensive information operations is to keep our information 'volume' from being

[24] John Garstka, "Network Centric Warfare: An Overview of Emerging Theory", *PHALANX Online,* December 2000 Volume 33 Number 4, http://www.mors.org/publications/phalanx/dec00/feature.htm (accessed 3 March 2003).

[25] As defined in Joint Pub 3-13, GL-7.

compressed."[26] Consequently, IO may be conducted both offensively and defensively. Offensive IO includes activities like "operations security (OPSEC), military deception, psychological operations (PSYOPS), electronic warfare (EW), physical attack and special information operations (SIO) and may include computer network attack."[27] Although offensive IO are conducted primarily through the physical and information domain, their prime target are in the cognitive domain - namely the human decision maker. Commanders will employ offensive IO influencing their adversary's observation, orientation and perception in order to cause responses that will be advantageous to their own military objectives.[28] On the defensive side of IO the objectives are two-sided. One is to minimize friendly IO system vulnerabilities to adversarial efforts and the other is to minimize friendly mutual interference during the operational employment of IO elements and capabilities.[29] Defensive IO includes activities such as "information assurance (IA), OPSEC, physical security, counterdeception, counterpropaganda, counterintelligence, EW and SIO."[30]

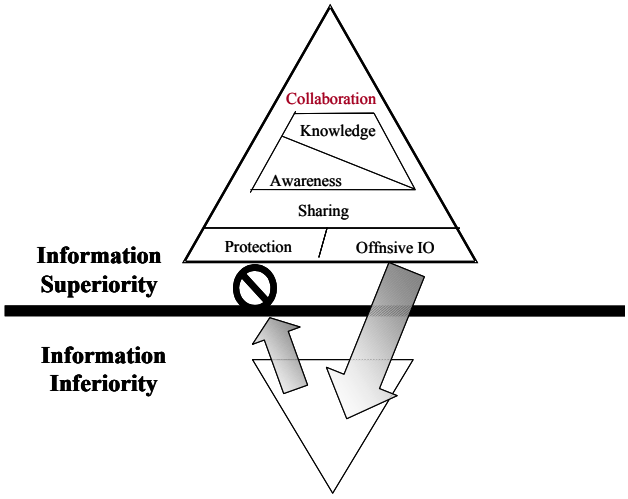

Figure 5. Elements of Information Superiority (From Alberts and Garstka, Dec 1999)

[26] Alberts, Garstka, Stein, Network Centric Warfare, 55.
[27] Joint Publication 3-13, viii.

[28] Dan Kuehl, "Information Operations: The Hard Reality of Soft Power." Joint Forces Staff College http://www.jfsc.ndu.edu/schools_programs/jciws/iw/io_textbook.pdf (not dated), 62 (accessed 18 May 2004)

[29] Kuehl, 41.

[30] Joint Publication 3-13, viii.

Figure 5 illustrates how IO is a basic element to achieve IS. Some of the fundamentals of IO are that it capitalizes on the current advances in information technology in addition to adapted doctrines and new forms of organizations. Increasingly more sophisticated computers, multiple and high speed connectivity and advanced networks enable IO to target information and information systems more efficiently. The goal is to affect human or automated based information processes.

The increased access to information takes place in three information infrastructures simultaneously: the global information infrastructure (GII), the National information infrastructure NII and the Defense information infrastructure DII. The GII is the "worldwide interconnection of communications networks, computers, data bases, and consumer electronics that make vast amounts of information available to users."[31] NII is similar to GII but related to a national information environment, while DII is deeply integrated in NII.[32] DII is the means, people and organizations that connect and support the armed forces' missions at all levels. However, it is not the volume of information itself that creates an advantage. Information overload constitutes a problem in itself and information can still be poorly used by decision makers. Consequently, changes in the information structure must be followed by doctrinal and organizational changes as well.

Furthermore, understanding the nature, complexity and dependencies between the information structures are crucial to exploit the opportunities the structures entail. Information Operations has a promising future to influence this relationship because it functions as an enabler that can shape the operational environment. Viewed as a process, IO can synchronize, synergize and deconflict activities in the information structure that ultimately will support the strategic, operational and tactical use of military forces.[33]

It is equally important to understand the vulnerability that comes with sophisticated computer systems, networks and the dependencies between the information structures. Studies of recent conflicts show that cyber attacks are becoming frequently

---

[31] Joint Publication 3-13, I-13.

[32] Ibid., I-14.

[33] Kuehl, 6.

more used as a part of the contending parties' arsenal in both conventional and unconventional conflicts. Countries like Libya, China, North Korea, Cuba and Russia, amongst others, are in the process of developing cyber warfare capabilities.[34] In addition, terrorist organizations, sympathizers, and different hacker groups, more or less with the consent of hosting nations, are also developing cyber capacities that have the potential of inflicting substantial damage to Western information systems, communications and infrastructure in future conflicts. These issues will be considered later, but to counter these threats and to defend our own information and information systems IO plays an important part through activities such as Computer Network Defence (CND) and IA. Two other contributors available to commanders, in order to achieve information superiority, are Intelligence, surveillance, and reconnaissance (ISR) and Information Management (IM). ISR and IM will not be discussed in detail here, but together these contributors enable and complement full spectrum dominance operations[35].

C. NETWORKING AND SYNCHRONIZING THE FORCE

As mentioned before, developments in IT, combined with organizational networking a force, is expected to provide access to a new, previously unreachable region of the information domain characterized by both increased information richness and information reach. However, there is no precise definition or ideal model within the NCW theory of what this network might look like. Webster's Online Dictionary defines a network as an interconnected or interrelated chain, group, or system. Within the organizational theory in general, network has often been seen as a level of analysis above the organizational level where some of the topics of interest are: how tight or loose coupled are the links; strength of ties; regulatory functions; scope and diversity of organizations in network; network persistence; and power centers.[36] In terms of networks as an organizational design Arquilla and Ronfeldt describe a network as "…dispersed "nodes" who share a set of ideas and interests and who are arrayed to act in a fully

[34] Trustees of Dartmouth College. "Cyber Attacks During the War on Terrorism: A Predictive Analysis." (Dartmouth College: Institute for Security Technology Studies, 22 September 2001), 12.

[35] Field Manual No 3-0 (FM 3-0), "Operations," (Headquarters Department of the Army, 14 June 2001), 11-11.

[36] Charles Perrow, *Complex Organizations: A Critical Essay.* (New York: McCraw-Hill, 1993), 195.

internetted 'all channel" manner.'[37] Furthermore, Arquilla and Ronfeldt refer to basically three types of networks: the chain, the hub and the all channel network. Although not stated in NCW literature, the type of network a NCW concept is reaching for is as complex as the latter, and it is "also the most difficult to organize and sustain, partly because it may require dense communication"[38]

An emerging approach for command and control in the information age and networked organizational structures is the so called *power to the edge* concept. Within NCW, *power to the edge* is considered a necessary condition for the networked force to reach a self-synchronizing capability. In Alberts' and Hayes' words, *power to the edge* is about:

> …changing the way individuals, organizations, and systems relate to one another and work. *Power to the edge* involves the empowerment of individuals at the edge of an organization (where the organization interacts with its operating environment to have an impact or effect on that environment) or, in the case of systems, edge devices. Empowerment involves expanding access to information and the elimination of unnecessary constraints. For example, empowerment involves providing access to available information and expertise and the elimination of procedural constraints previously needed to deconflict elements of the force in the absence of quality information. Moving power to the edge implies adoption of an edge organization, with greatly enhanced peer-to-peer interactions. Edge organizations also move senior personnel into roles that place them at the edge. They often reduce the need for middle managers whose role is to manage constraints and control measures. Command and control become unbundled. Commanders become responsible for creating initial conditions that make success more likely and exercise control by:
>
> - Creating congruent command intent across the enterprise;
>
> - Allocating resources dynamically; and
>
> - Establishing rules of engagement and other control mechanisms that the fighting forces implement themselves. [39]

Thus, a network-centric force consist of empowered, interoperable, self-synchronizing entities that provides commanders with the capability to dynamically

[37] John Arquilla and David Ronfeldt, *Networks and Netwars,* (Santa Monica: RAND, 2001), 7.

[38] Arquilla and Ronfeldt, *Networks and Netwars,* 9.

[39] Alberts and Hayes, *Power to the Edge,* 5.

network (connect, share, and collaborate) the three main sets of battlefield components: sensors (regardless of platform), decision-makers (regardless of location) and shooters (regardless of service). Each component in the net may consist of an individual, an entity/organization or a type of technology or materiel.

The sensor component has sensing as its main function and contributes to knowledge of the battle space. It encompasses all components, from satellites to an individual's sight, which contribute to awareness and understanding. The decision component typically decides the allocation of resources, sets the priorities, and reconfigures the organizational structure based on the current situation awareness established by interpretations from the sensing process. The shooter, or transaction, component's main function is to affect the situation or target by some type of action by lethal or non-lethal means.

According to Alberts and Hayes, the basic tenets of NCW begin with the existence of a robustly networked force, and interoperability among the different networked entities are substantial.[40] This applies to all levels or layers in the structure.

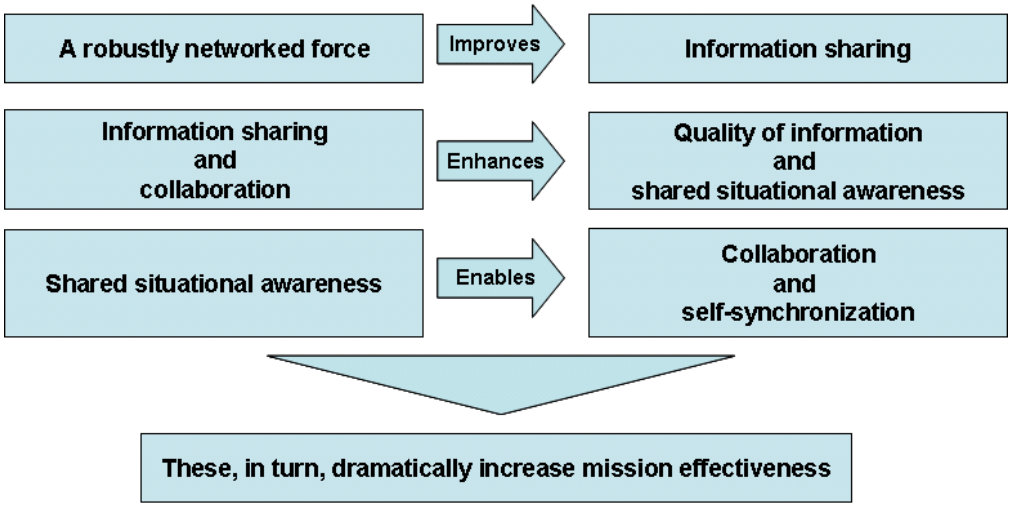

Figure 6. The Tenets of NCW (From Alberts and Hayes, June 2003)

Interoperability must be present within all four domains: physical, information, cognitive and social. The degree of interoperability within these domains determines an

[40] Alberts and Hayes, *Power to the Edge*, 107.

entity's ability to perform NCW operations. With reference to the four domains, entities in a network need to…

1. be connected to the net
2. be able to provide information to those on the net
3. be able to find, retrieve, and understand the information available on the net
4. participate in one or more virtual collaboration environments or processes

…to increase the value of information in the net.[41] The profit of a network centric concept, as compared to platform centric, is the increased value and availability of information about the battle space provided by the sensors combined with the connections, or multiple links between the different components within all four domains. This increased situational awareness at all levels gives an opportunity to rapidly respond, reallocate or shift focus as the situation changes. Moreover, the idea is that ownership of each component (e.g. weapons and sensors) should no longer be integrated or organically belong to one particular decision maker or a single platform. Instead, the components work together sharing information and exploiting changes in the situation according to the commander's intent. The result is a dynamic organization reacting to the changing situation by a continuous reconfiguration of available forces made to fit to the highest prioritized missions.[42]

D. CONCLUSION

The highest degree of maturity in a NCW force is when all the entities in the net have a fully shared awareness and are able to truly self-synchronize their operations. At the bottom lies a fully developed doctrine for warfare in the information age together with new types of organizational structures. Ultimately, the side that possesses the best information and manages to transform it to shared awareness and subsequent synchronized and timely actions achieves a major advantage versus its opponent. That is, concisely, the prospect of a NCW concept.

---

41 Alberts and Hayes, *Power to the Edge,* 107.

42 Norwegian Chief of Defense, "Konsept for nettverksbasert anvendelse av militærmakt."

III. NORWAY'S STRATEGIC ENVIRONMENT

Seen from a power-based theory, small nations have many constraints shaping their security and defense policies compared to larger and more resource-rich countries. Although it is aimed at an individual or an organization, Charles Perrow's definition of power as "the ability of persons or groups to extract for themselves valued outputs from a system in which other persons or groups either seek the same outputs for themselves or would prefer to expend their effort toward other outputs,"[43] is useful also to explain state-to-state relationships. The key is that power based on diplomatic, economic, military or psychological resources always has been used to secure, alter or distribute a nation's various outputs. This could be substantial outputs such as sea or land territories, natural resources or other trade products, or more abstract outputs in the form of ideological, philosophical and political ideas.

Arguably, and due to its smaller power base, a small nation's strategic environment is to a larger extent determined by world events and larger nations' leniency more than its own influence. Hence, historically for Norway, a constrained approach to the use of statecraft, particularly the use of psychological (informational) and military means, have been deemed more fit than a proactive and offensive strategy using all means available. The exception was perhaps the Viking era (750-1100) where the Vikings' culture and military power strongly influenced the British Isles as well as continental Europe as far south as Constantinople. In modern time, Norwegian activities and interests are even more global, especially within the maritime cluster in sectors such as shipping and ship building, oil and gas exploitation, the cruise liner business and in the whaling and fish industry. However, these activities have developed more or less independent of Norway's state power as such. The outputs of these activities have never been linked to an overall national strategy, which also integrates political and military elements. The need for such a strategy that also encompasses Norway's military doctrine, has been raised by many scholars.[44] In this view, developing a NCW concept in the

[43] Charles Perrow, 259.

[44] Amongst others by Iver Neumann in "Norges handlingsrom og behovet for en overgripende sikkerhetspolitisk strategi". http://www.atlanterhavskomiteen.no/publikasjoner/sp/2002/3.htm (accessed 24 March 2004).

Norwegian military cannot and should not be initiated without the appropriate strategic context in which it is supposed to support and defend Norway's interests. Furthermore, these interests may be different from the common interests of NATO, the single most important cornerstone in Norwegian security since the Organization's origin. In addition, other important strategic features of Norwegian society play an important part. This chapter will explore these features in the strategic environment and the implications for military transformation in a NCW direction.

A. STRATEGIC FREEDOM OF MANEUVER

Norway's security is, in an as yet incalculable future, linked to the power triangle between the United States, the European Union and Russia. This dependency was also recognized in 2000 when the Norwegian MoD proposed the most extensive reorganizing of the armed forces since WW II:[45]

- Norway's security is highly dependent on the member states' continued commitment to NATO.
- Norway should contribute to preserve and strengthen NATO both politically and militarily and thereby also secure continued transatlantic cooperation.
- Norway should actively participate in the development of the crisis management mechanisms in the EU.
- Norway should actively ensure that Russia is included further in the European and broader international security and defense environment.

Summarized in Figure 7 is the influence of the larger powers and Norway's freedom of maneuver in security affairs. The latter is limited and dependent on the triangle's three centers of gravity. A gradually stronger Russia that seeks influence may entail a potential increased pressure against Norway; in particular for those cases where Norway and Russia have conflicting interests, such as in the maritime limits between the two countries in the Barents Sea and also Russia's challenge of Norwegian jurisdiction beyond Svalbard's territorial limits within the Svalbard Treaty. Increased pressure from Russia will reinforce the dependency on NATO/EU, or alternatively, it will require a greater capability for independent crisis management

[45] Norwegian MoD, St.prp nr. 45 (2000-2001), "Omlegging av Forsvaret i perioden 2002-2005", *19*

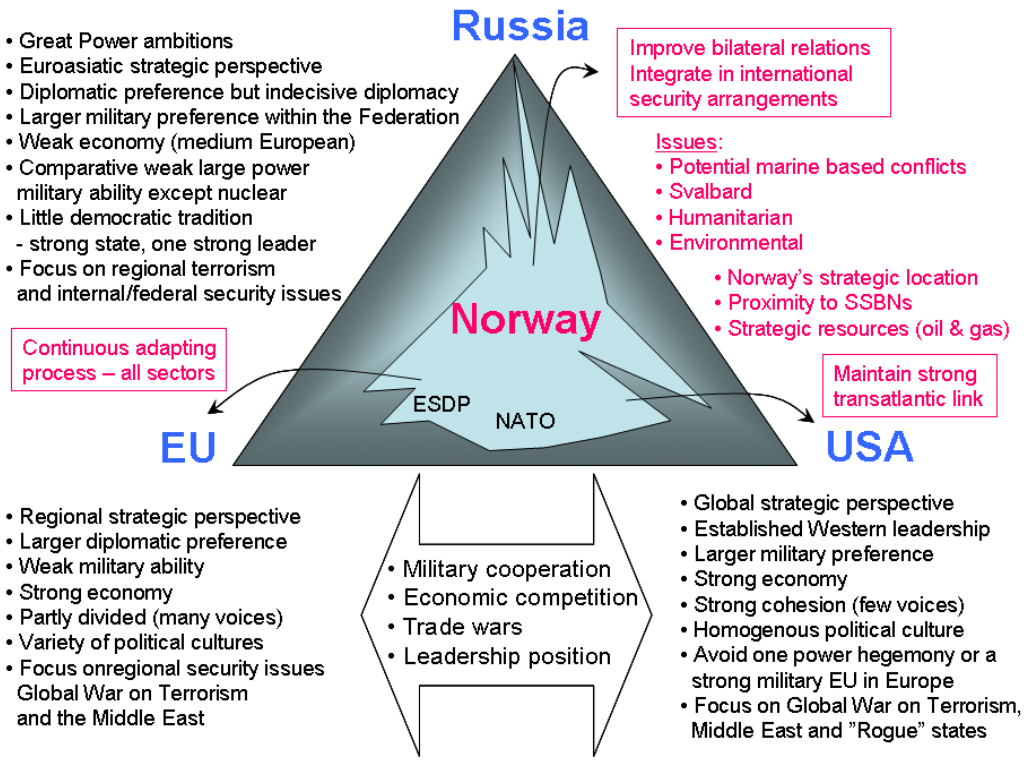

Figure 7. Power Triangle and Strategic freedom of Maneuver

Another challenge for Norway's security policy is the marginalization that takes place on at least three levels.[46] First, is the Nordic region where the focus has shifted from the Norwegian Sea/North Sea to the Baltic region. Secondly, on the European level, where Norway as a non-member state never can be integrated into the EU's common security and defense policies. On the contrary, without full partnership Norway will be regarded as a competitor to the EU, particularly in the trade and economic sectors. Lastly, it is marginalization at the transatlantic level where the development of NATO increasingly takes place through a U.S.-EU dialog. Practically, Norway tries to balance its policy between the three powers' main goals as depicted in Figure 7. This is often a delicate balance where Norway avoids making obvious choices between the EU and

[46] Bjørn Knutsen et al. "Europeisk sikkerhet i en foranderlig tid: En analyse av Norges utenriks- og sikkerhetspolitiske handlingsrom", The Norwegian Atlantic Committee, *Det sikkerhetspolitiske bibliotek nr 4 – 2000,* http://www.atlanterhavskomiteen.no/publikasjoner/sp/2000/4-2000.htm (accessed 26 March 2004).

NATO.[47] Apparently, this has not become an easier task recently in the wake of the Iraqi war. According to a new comprehensive study of transatlantic trends,[48] there is growing European criticism of the alleged U.S unilateralism and global leadership, the preferred means and institutions (e.g. the UN) to deal with international crisis, and the willingness to spend resources on the military. Americans share European concerns about U.S. unilateralism, but have a larger willingness to bypass the UN if required by national interests. In addition, the U.S. wants the EU to be a stronger partner with which it can share common and global responsibilities.

In light of this increasing rift in transatlantic relations it is perhaps an even more important security issue for Norway to contribute to transatlantic cooperation. However, the situation also calls for a re-evaluation of what many used to take for granted; an automated transatlantic or allied reinforcement if a conflict should emerge. In a less cohesive alliance there might not be a larger network to plug into during a limited conflict between, for instance Norway and Russia. Consequently, Norway must also secure a certain capability to act alone in case of a crisis where neither of the two security institutions is willing or able to support distinctive Norwegian interests. In addition, since both institutions seek a tighter integration of Russia in the security policy arena, such a conflict in the northern region may be too small for the larger powers compared to the political strain of getting involved.[49] This problem could partly be solved by increasing Norway's power base, both militarily and economically through EU membership. However, Norway has turned down this question in two referendums (1972 and 1994) and is obviously still not ready to make that commitment partly because it implies the submission of some of its sovereignty to the Union, in addition to a greater sharing of the natural strategic resources Norway so strongly depends upon. As a consequence, and to a much larger extent compared to other similar sized countries within NATO and the EU,

---

[47] Iver Neumann, "Norges handlingsrom og behovet for en overgripende sikkerhetspolitisk strategi" The Norwegian Atlantic Committee*, Kort-info fra DNAK 1-2001,* http://www.atlanterhavskomiteen.no/publikasjoner/andre/kortinfo/2001/1-2001.htm (accessed 26 March 2004).

[48] Findings from Transatlantic Trends 2003. After a public opinion survey undertaken by the German Marshall Fund of the United States (GMF) in Washington D.C., USA, the Compagnia di San Paolo in Turin, Italy and the Luso-American Foundation in Lisboa, Portugal. http://www.transatlantictrends.org/ (accessed 3 Mars 2004).

[49] Neuman, 4.

Norway's development towards a NCW concept has to ensure a certain capacity for independent crisis management. This does not imply that Norway should aim to match a future Russian threat by itself; however, it does imply a requirement for gaining a political/military initiative and leadership in the northern region as well as having a continuous military presence in the area. Thus, national needs must be reflected in a NCW implementation strategy as well as fulfillment of the NATO/EU requirements for military transformation.

Moreover, homeland-defense proponents would reasonably argue that a development of tailored NCW capacities for domestic purposes should have precedence over the new and "exported" security requirements. This discussion, which is both politically and military relevant in the ongoing transformation process, most likely can only find its solution based on a comprehensive national security strategy. Until such a strategy is in place, regional and local political interests, and inter-service rivalry will continue to disrupt a purposeful transformation of the military forces towards better ends in the information age. Besides, by not thinking nationally and independently, Norway misses the opportunity to develop a NCW concept that fits the distinctiveness of its smaller power base. This approach to Norway's power base might focus on other valuables of NCW such as doctrinal and organizational issues rather than costly technology which, some think have had a too prominent place in the Norwegian NCW debate until now.

B. THE NATO UMBRELLA

Emphasized in NATO's new strategic concept is the new and uncertain security environment. However, the uncertainty is based on a less existential threat than that endured in the Cold War. With the disappearance of the communist threat, the U.S. and NATO directed their political and military attention and resources to other problems, symptoms of violence, or conflicts throughout the world. Earlier, minor and mostly intrastate conflicts functioned as surrogate wars between the two military blocks where ideological views determined the political agenda and the invested resources. The new security environment, however, has led to an expansion of the NATO military task list, including peace support operations and the fight against terrorism, crime, for human

rights and environmental issues.[50] Not only have these problems been defined as security threats directly linked to Norwegian security interests, but the political will to use military power to resolve them has increased significantly. In 1999, Norway terminated a 21 year long commitment in Lebanon under the U.N. flag where more than 34, 000 Norwegian soldiers have participated. In addition, since 1990 Norway has participated in most major conflicts from the first Gulf War, to the conflicts in the Balkans, then in Afghanistan as part of the U.S. led operation Enduring Freedom and also in the International Security and Assistance Force (ISAF) troops. Most recently is the small but politically disputed engagement in Iraq where Norwegian forces are contributing to provide security and humanitarian assistance in the post-conflict phase.

In addition to an increased will to use its military power, NATO's security boundaries are now theoretically unlimited. This is in sharp contrast to the Cold War period where the military power of NATO never was to exceed NATO's well defined boundaries by going "out of area." The discussions of out of area operations within NATO are now long gone, as described in the 2002 Prague Summit declaration:

> We are determined to deter, disrupt, defend and protect against any attacks on us, in accordance with the Washington Treaty and the Charter of the United Nations. In order to carry out the full range of its missions, NATO must be able to field forces that can move quickly to wherever they are needed, upon decision by the North Atlantic Council, to sustain operations over distance and time, including in an environment where they might be faced with nuclear, biological and chemical threats, and to achieve their objectives.[51]

Consequently, since Norwegian security is tightly linked to NATO, the Norwegian security focus has shifted from NATO and homeland defense to include more peripheral security requirements abroad. This strategic shift in the use of military power has caused a widespread political and military debate contrary to the across party lines agreements in defense policies experienced in Norway since WW II until the early nineties. One of the main issues is the quantity and relevance of the armed forces for

---

[50] NATO, The Alliance's Strategic Concept. North Atlantic Council in Washington D.C. on 23rd and 24th April 1999. <http://www.nato.int/docu/pr/1999/p99-065e.htm> (accessed 17 September 2003).

[51] NATO, Prague Summit Declaration, paragraph 4. http://www.nato.int/docu/pr/2002/p02-127e.htm (accessed 25 Feb 2004).

homeland defense purposes in a transformation process that apparently is focused to fulfill NATO needs and requirements. Hence, the Norwegian Minister of Defense, Kristin Krohn Devold, continuously must reassure the Norwegian parliament that the usability of a transformed structure fits both needs. Her argument to prioritize allied requirements is most valid; "If Norway ever needs support from NATO, our forces have to be interoperable with our supporters. And, if any other NATO countries need support from Norway, our forces must be interoperable with the supported forces."[52] However, doubts about the reduction of mass and absence of forces in areas that earlier was considered vital for Norway's security interests is still a concern; but it seems that the MoD's view are becoming more and more prevalent.

How valid is the perception of the opposition that a shift of focus from territorial defense to an exported security policy is a dismal decision? It appears that the disagreements go along three lines of strategic argument. First is the likelihood of an invasion or larger military dispute on the Northern Flank. In today's security environment, most security analysts and politicians in Norway see this likelihood as very low. On the other hand there is also uncertainty connected to Russia's development:

> Russia remains, in terms of both its short- and long-term fate, a fascinating and somewhat terrifying puzzle to the West. Declines in personal income, personal safety, and life expectancy have created political volatility and ripe opportunities for extremists of every sort. Moreover, for the foreseeable future, Russia could at any time become again the decisive factor in determining American engagement in European and even global security matters.[53]

Since 1996, when the above citation was written, Russia has had clearly positive domestic developments and has also returned as a stronger security policy actor both globally and in Europe. The problem, however, is that it is not clear in which direction Russia wants to use its influence. It could either seek European integration or remain a

---

[52] Kristin Krohn Devold,: *Usability through transformation* Speech at the Norwegian Atlantic Committee's "Leangkollen" conference. 2 February, 2004. http://odin.dep.no/fd/engelsk/aktuelt/taler/statsraad_a/010001-990096/index-dok000-b-n-a.html (accessed 25 Feb 2004).

[53] Richard Leone in Michael Mandelbaum, *The Dawn of Peace in Europe* (New York: The Twentieth Century Fund Press, 1996), viii.

transatlantic actor.[54] Russia has also become more authoritarian under Putin's regime but this may be considered as a stabilizing factor so far. Nevertheless, it could be wise to still factor in some uncertainty with regard to Russia's development.

Linked to the likelihood of military confrontation is the probability of receiving allied support. Clearly, in an Article Five scenario, NATO support can be expected. Hence, it is support in a minor crisis that can be disputed, however, it may look minor in the eyes of NATO or the U.S. but it can be relatively consequential for Norway as a small nation.

Secondly, there is a question of predictability and timeframe for the defense planning in NATO. Will a NCW concept meet Norway's short and long-term security requirements? Implicit in the ongoing transformation process is a shift from a long-term planning perspective of 20 – 30 years[55] towards dynamic incremental improvements in a NCW direction where the planning horizon is in terms of years rather than decades. In the U.S. DoD's Office of Force Transformation the reduced planning horizon, based on a uncertain future in the information age, is called *rapid spiral transformation.* This approach is focused on "…rapid, incremental changes to exploit improvements in technology, processes and organizations that contribute to larger jumps in concept and capabilities. Taking a large number of small-to-medium exploratory jumps, risks are low, but the payoffs quickly accumulate."[56] The question is whether the risk of reducing Norway's military presence and capabilities in its northernmost areas can be considered a low-risk venture, considering the still unpredictable developments of its mighty neighbor Russia.

The third concern is if the planned NCW concept will provide the proper type of forces and a sufficiently large force structure to secure and manage Norway's enormous wealth of natural resources. Most of these resources are marine resources such as oil, gas

---

[54] Iver Neumann and Kristine Offerdal, *Russia is Back.* The Norwegian Atlantic Committee, Internett tekst nr 18, November 2003. http://www.atlanterhavskomiteen.no/publikasjoner/andre/i-tekster/18.htm (accessed 24 March 2004).

[55] This planning timeframe typically coincides with the development, procurement and implementation of major military material such as submarines, NATO frigates, etc.

[56] John Hanley, *Rapid Spiral Transformation*. DoD Office of Force Transformation, Transformation Trends – 3 February issue 2003.http://www.cdi.org/mrp/transformation-trends.cfm (accessed 26 Feb 2004).

and fish in an area that is seven times the land territory, covering the North Sea, the Norwegian Sea, the Barents Sea and the adjacent waters surrounding Svalbard. The latter is a Norwegian protectorate in accordance with the Svalbard treaty of 9 Feb 1920. The fact that the marine resources represent nearly 50% of the Norwegian GDP[57] underlines the dependency and importance for Norway to manage and protect them accordingly.

Arguably, being under the U.S. and NATO security umbrella for almost 40 years has in many ways spoiled the Norwegian population's view of what the demands really are for protecting these offshore resources and state investments against, for instance, rogue states and terrorism. In this sense the Norwegians are not alone, or as expressed by Robert Kagan:[58]

> Europeans have generally believed, whether or not they admit it to themselves, that whenever Iraq or some other rogue nation emerged as a real and present danger, as opposed to merely a potential danger, then the United States would do something about it. If during the Cold War Europe by necessity made a major contribution to its own defense, since the end of the Cold War Europeans have enjoyed an unparalleled measure of "free security" because most of the likely threats emanate outside Europe, where only the United States can project effective force."

Kagan's statement may be nuanced in light of the many instances where European countries indeed have taken care of their own security far beyond their borders,[59] and must be seen in relation to the transatlantic rift that emerged in wake of the Iraqi intervention. Nevertheless, in a larger perspective, the Norwegian welfare state and prosperity was allowed to expand almost unaffected by Russia's or other nations' influence or intervention during the Cold War period. Certainly there were disputes, particularly with Russia, and many of them are still unresolved,[60] but it can be speculated that there were considerable restraints from the negotiating parties in order not to exacerbate any situation that could involve interference in a bipolar context. Moreover, disputes were never allowed to create reasons for skirmishes of any type. This situation

[57] Figures derived from 2001 numbers. Statistics Norway *Gross domestic product, by kind of activity* http://www.ssb.no/english/subjects/00/minifakta_en/en/ (accessed 26 Feb 2004).

[58] Robert Kagan, *Of Paradise and Power* (New York: Alfred A. Knopf, 2003), 33.

[59] For instance, the British during the Falklands War, Germany's counterterrorism operations in Mogadishu, and the many preemptive operations by the Israelis to defend their immediate security interests.

[60] For instance, the Norwegian-Russian dispute on maritime borders.

was not only positive with regard to Norwegian claims because, as a small country, Norway felt an immense responsibility not to evoke a situation between the superpowers based on its sole economic interests. Thus, the Norwegian freedom of maneuver in these questions was also very limited. Today, they are still limited but the strategic choices rest more independently on Norway's own power base. As a result Norway must develop strategies to look after its own interests based on individual means of statecraft. This includes diplomatic, economic, informational and military strength. For these reasons it could be argued that Norway's requirements for self-sustaining security measures have increased and not decreased since the discontinuation of the Cold War. The larger question for the military is, however, how to efficiently support such a policy in the ongoing transformation process. Part of this answer can perhaps be found by exploring the specific interests that are at stake.

C. THE IMPACT OF INTERESTS

Central in the strategic environment are the particulars of the interests related to a country's security, values, legitimacy, welfare and economic basis. To optimize a NCW implementation, the national interests should be analyzed and balanced against Norway's strategic freedom of maneuver previously discussed. The conclusions of such an analysis can function as guidance regarding what to prioritize in the military transformation process. Questions that ought to be answered are for instance, what interests are threatened and how important are they? What interests will influence the dimensional factors of the military structure? In what environment do the most important interests occur? Are they sea or territorial based, regional or global? What type of technology can best meet the challenges in these environments? What type of strategic and operational concepts will be suitable? How should the services be prioritized to meet the requirements?

For Norway's part, without an overall national security policy strategy it is difficult to get a comprehensive understanding of the strategic interests, their prioritized order and their impact on military affairs. It is symptomatic for the situation that the greatest successes for Norwegian foreign policy in the last decades has been as a peace arbitrator based on the perception that Norway has few interests and a negligible

capability to influence the comparative strength between two adversaries.[61] The abstract interest of preserving a reputation as a peace arbitrator is honorable and valuable in order to preserve global peace, but it may also contribute to suppress Norway's more substantial interests. These interests are not always obvious to the public because they are found in multiple departmental strategies and initiatives. The span of interests is not always reflected or easily found in the defense policy.

Typically, the Norwegian Chief of Defense receives political guidance from the MoD, and it includes a thorough analysis and description of changes and threats in the overall security environment. However, the conclusive assessments are superficial and generate very broad tasks for the armed forces. An overview of the total set of current security and defense policy objectives and the subsequent tasks is depicted in the following table.[62] They are also repeated in the Chief of Defense's latest study with the intent to advise politicians about the future defense policy and structures.[63]

---

[61] Tore Nyhamar, "Norske Nasjonale Interesser I Nord-Atlantaren" *The Norwegian Atlantic Committee Internet text nr. 11- 2003*. http://www.atlanterhavskomiteen.no/publikasjoner/andre/i-tekster/11.htm (accessed 16 March 2004).

[62] MoD, *Norwegian Defence 2004.* Online fact book on the Norwegian defense. http://odin.dep.no/fd/engelsk/publ/veiledninger/010011-120064/index-dok000-b-n-a.html (accesses 5 March 2004).

[63] Chief of Defence *Forsvarssjefens Militærfaglige Utredning 2003* (Oslo: 2003).

Security Policy Objectives	Defense Policy Objectives
– To prevent war and to contribute towards stability and peaceful development, including the prevention and combating of terrorism – To safeguard Norwegian rights and interests, and to protect Norway's freedom of action in the face of military or political pressure – To uphold Norwegian sovereignty – To protect Norwegian land, sea and air territory against incursion and attack	– The maintenance of military presence and visibility – The ability to produce and exchange risk assessments and early warnings – The ability to deal with incidents and crises – The ability to defend Norwegian land, sea and air territory against military attack – The ability to operate jointly with allies and to take part in international force structures and operations – Participation in defense-related cooperation with other countries and within international organizations
Defense Concept	**Military Defense Tasks**
– A balanced and flexible national defense – Operating jointly with allies and participating in international defense cooperation – Total defense and other civil-military cooperation – Compulsory military service	– Maintaining a military presence in priority areas – Upholding national sovereignty and the exercise of national authority – Crisis management in areas under Norwegian control – Defending Norwegian territory and preparing, together with allies, to meet any challenge to Norwegian security – Securing facilities and activities that are vital to Norwegian society – International involvement – Being of use and assistance to society at large

Table 1. Norwegian Security and Defense Policy

As shown in the Table the political and military goals, objectives and tasks are very general in nature. Although, they are elaborated further in the original documents, and particularly measured against the recent developments in security and defense policy such as the new global security situation, asymmetric threats, cyber threats, terrorism, and advances in information technology, they are not interest specific and it is problematic to sort out where the important challenges are.

Perhaps this uncertainty is one of the most characteristic features of security policies in the new century. Nobody seems to know what the future will bring, but there

are many good but conflicting assessments[64] in addition to a lot of guessing. However, even if interests may change rapidly in the new world order, many of Norway's interests are, in fact, very stable due to Norway's geopolitical situation. Especially in an uncertain environment, it would be wise to actively focus more on these interests. Both politically and militarily there has been little tradition to do so. Less use of public diplomacy and a careful appearance within international institutions have been the preferred course of action. Arguably, that makes sense for a small country because many of the interests in question depend on international law and cooperation. On the other hand, the interests remain relatively unknown to the public, not only internationally but also domestically. This general political guidance is problematic for several reasons:

- The security policy analysis does not always create the *logical link* between current and future threats to the specific interests that needs to be secured or defended.
- Except for the existential and allied interests, an inconclusive and general security policy does not give a *clear signal* to the military, or an adversary, about which interest there is a political will to defend, and as a consequence…
- It becomes difficult to develop a *comprehensive military strategy* that has a *deterrent effect.*
- It becomes difficult to orderly *prioritize or develop the necessary capabilities* to meet the political demands when the need to protect the interests arises.

In sum, the direction of important military affairs, such as the ongoing military transformation, becomes unclear. There is too much room for interpretation of the political ends which ultimately also leads to a subsequent, more difficult, debate on the means and ways to reach them.

As an example of how a further specification of interests might be useful in the transformation process is a systematic analysis of the Norwegian national interests in the North Atlantic region made by Tore Nyhamar at the Norwegian Defense Research Institute. National interests, in this assessment, are determined by the dynamics and consistency between four conditions:[65]

---

[64] For instance, see Martin van Creveld in the *Transformation of War* (Free Press, 1991) versus Harry G. Summers in *The New World Strategy* (Touchstone, 1995) for different views on the nature of future conflicts and use of military forces; and Michael O'Hanlon in *Technological Change and the Future of Warfare* ((Brookings, 2000) versus Admiral Bill Owens in *Lifting the Fog of War* (FSG, 2000) with regard to diverging views on RMA hypothesis and the impact of technological change.

[65] Tore Nyhamar, *Norske Nasjonale Interesser I Nord-Atlanteren.*

- a set of core interests
- a set of derived interests
- a set of derived strategies or policies
- a set of facts or relevant background theory

Based on this dynamic interaction of identified core and derived interests, theoretical or practiced strategies and policies, Nyhamar lists the Norwegian national interests in the North Atlantic as follows:

Vital interests (secure and increase the welfare of the people in a free and secure state)
– Protect Norway against a foreign will brought upon the country by force – Maintain and develop a security policy alliance based on common interest in such a way that we will not stand alone in a conflict with Russia – Maintain a trustworthy ability for exercising an authority that entails international acceptance (includes physical capabilities and the perception of others that the exercise of authority is objective and legitimate)
Very important interests
– Promote Norwegian economic interests, including: o beneficial use of fishery resources in the North Atlantic o beneficial use of the petroleum resources in the North Atlantic o Safe passages in the Norwegian adjacent waters – Maintain and develop international institutions (e.g. maritime law) in order to avoid a bilateralization of the situation with Russia – Promote the understanding that the oceans under Norwegian jurisdiction are an important interest and that Norway's management of these areas is a common good – Preserve the environment in Norwegian adjacent waters, including: o avoidance of oil pollution from oil industry and oil tankers o avoid radioactive pollution from radioactive waste and reactors – Maintain and develop strong regional organizations for crisis management – Maintain and develop a strong and relevant UN
Important interests
– Stability in Russia – Promote democracy and a civilized society in Russia

Table 2. Norwegian Interests in the North Atlantic

The impact of the above identified interests can be important in a NCW implementation context for several reasons.

First, since the basis for Norwegian defense is no longer tied to an existential threat from the East, but rather to defend a broader range of national and allied interests,

it is imperative that these interests are well identified and specified in order to develop matching NCW capabilities. U.S or NATO NCW blueprints might not fit the Norwegian needs very well.

Secondly, although Russia no longer represents an existential threat, it stands out as a great concern in most of the described interests. Hence, Norway's NCW capabilities should be organized to ensure a proper development of bilateral military and civilian cooperation, and in case of a crisis, also to meet potential means of coercion from Russian authorities or organizations.

Third, since the reach of NATO has turned global, and to a larger extent is following a U.S or EU interest base, it would be naïve to believe that the use of Norwegian military power in an allied or coalition context will always be concurrent with Norwegian interests. Despite the growing transatlantic rift and the political turbulence that followed the Iraqi intervention, the greater powers' foreign policies have been in Norway's interest so far, but what about the future?[66] Allied cohesion is extremely important for Norway and it is also fair that its foreign policy, to a certain extent, supports the U.S. and larger nations' national security interests, especially since the former are contributing proportionally larger resources in the Alliance. However, reasonable arguments must be raised in an institutional manner when conflicting interests arise. In a globalized but interest-based world, Norway's particular interests will be more respected as long as they are visible, well-founded and balanced toward the common good. In short, Norway must, to a much larger extent than before, take care of its own interests both independently and within the Alliance. That might require different approaches to the NCW concept and connected capabilities.

Fourth, specifying the interests gives direction and prioritization of the needed capabilities in a NCW implementation. For instance, Nyhamar's analysis would suggest that Norway should:

- Continue to develop allied relations and relevant NATO NCW capabilities

[66] As an example Kagan (31) points to the different perception between the U.S. and Europe with regard to tolerance of repressive or threatening regimes. While the former refers to these regimes in terms of "axis of evil" and "rogue states" the latter tend to use terms as "failed states", which not only determines the threat they pose but also what instruments of statecraft, if any, should be used against them.

- Emphasize NCW capabilities that are maritime because a regional or local conflict in the future will probably be related to Norway's economic centre of gravity that currently is found in fishery and the offshore oil and gas industry
- Emphasize the development of an interagency network within the same maritime cluster that would enhance the government's ability to conduct crisis management in the northern region
- Prepare units in the armed forces for operations under the UN flag where standardization, interoperability, conceptual and procedural requirements may differ somewhat from those that are developed in a NATO context. In addition to allied NCW "plug in" capabilities, perhaps these forces should be prepared to *build* networks and enable non-allied countries to function under a Norwegian led "net" as well

The main point here is not to focus on Nyhamar's example but rather the necessity to taylor the development of NCW capabilities to Norway's long term interests accordingly. In this sense, Norway's security environment and long-term interests should be functioning as a driver for the NCW implementation.

D. ECONOMIC AND TECHNOLOGICAL PREMISES

So far in this thesis it has almost been an underlying condition that the development of NCW capabilities will demand radically higher defense spending in the future. With a continued emphasis on the technological side of RMA and the increased R&D costs for new military material, this assumption might be true. For instance, the concept of Information Superiority is anticipated to bring about a tremendous effort in the future to develop and implement new information technology on a broad scale to U.S. forces. Figures suggest that the U.S. "spends more on its information technology than all but a couple of great powers spend on their entire militaries."[67] Thus, there are serious concerns whether Norway or other allied forces will be able to communicate adequately and share information with the U.S. military in future conflicts. These concerns have already been addressed in NATO, first by the Defense Capabilities Initiative (DCI) and most recently in the Prague Capability Commitment (PCC). In these initiatives, the member states have agreed to pursue common efforts within certain areas to reduce the

67, Thomas P.M. Barnett. "The Seven Deadly Sins of Network-Centric Warfare." *Proceedings,* U.S. Naval Institute, January 1999.

gap between the U.S. and the European pillar in order to improve the Alliance's capability for modern warfare in a high threat environment.

Taking its share of DCI, PCC and similar initiatives[68] is important to Norway's credibility and usefulness in NATO. "Norway must contribute actively to the modernization of NATO. This means continuing to contribute relevant capabilities to NATO's structures and operations and making Norway's unique training facilities available to the Alliance."[69] Consequently, as NATO goes along in a NCW direction Norway is committed to follow. The problem is if NATO becomes less relevant as a defense alliance, due to increased politicization or increased gaps in doctrine or technology, it may no longer function as a defense alliance in minor crises or under non-existential threats.

To many, and despite the rapid article five declarations in NATO after the 11 Sep 2001 attacks, the U.S. decision to intervene in Afghanistan, within a coalition framework rather an allied one, serves as an example for this danger. This decision was made for several reasons.[70] First, the Americans wanted a broader coalition but the requirements for troops on the ground were low. Second, they wanted a higher level of political/military control and speed in the decision-making process than experienced in Kosovo. Third, the technical requirements of the intervention and the nature of forces and weapons employed limited meaningful allied contributions. In short, U.S. officials viewed allied support as politically useful but militarily insignificant. If this development continues, where diverging politics or the dependency on new technology enables only U.S. forces, or a few of its allies, to operate on the battlefield, it may critically damage the efficiency and cohesion of the Alliance. It will also limit a coalition of the willing. Alternatively, as experienced in Iraq, U.S. forces will be used as an enabling force conducting the "war-fighting" such as strategic bombing and the initial ground battles. Other forces will perhaps be sent in to secure the peace when the fighting is over or

---

[68] Other initiatives are managed through organizations within NATO such as the Multinational Interoperability Council (MIC), Combined Communications Electronic Board (CCEB), and the NATO C3 Board.

[69] Norwegian MoD, Proposition to Parliament No. 42 (2003 – 2004) English short version, 8.

[70] Tom Lansford, *All for One: Terrorism, NATO and the United States.*(Burlington: Ashgate, 2002), 110.

otherwise contribute to the operations; for instance with logistical resources or taking over responsibilities in other theatres where the situation is more secure. However, in the long run, such a policy will be damaging. Attention and debate regarding the legitimacy of a conflict will always peak when the conflict is most intense. An impression can be made of the U.S. as a unilateral and aggressive nation, pursuing its own interests, if it stands out singularly on the battlefield in the initial phase. In these cases NCW capabilities might help U.S. forces to win the battles, but if the U.S. becomes the scapegoat the peace might be lost. In addition, if the imbalance in military power continues, it is likely that the rift in the transatlantic link will continue to grow. It is therefore imperative to ensure that most allies have a role to play in future conflicts even if it plays out within a NCW concept.

Likewise, in case of a more existential conflict, such as a more tangible Article Five situation within NATO, cooperation and interoperability will be crucial from the outset. Without interoperability and a common situational awareness, the efficiency on the battlefields might actually decrease. The benefits of IS may diminish because the commanders intent cannot be distributed sufficiently down the chain of command. Also, the fear of "blue on blue situations"[71] may delay the decision making process and the shooters efficiency. Consequently, measures have to be taken when new IT is implemented within NATO to assure that the forces are able to operate on the same battlefields simultaneously. Inevitably, in an allied context IS has to be a shared superiority to be advantageous.

Nevertheless, there are alternative approaches to fund the ongoing RMA in a NCW direction. In an American transformation context, Michael O' Hanlon suggests four guidelines to further promote defense innovation within the current budget levels.[72] The first is to "emphasize relatively economical and high-payoff improvements in munitions, communications, information systems, and sensors that are possible today due to trends in electronics and computers."[73] In Norway, this aspect of economization is

---

[71] Expression used when inadvertently firing on friendly forces.

[72] O'Hanlon refers to the year 2000 budget. Michael O'Hanlon, *Technological Change and the Future of Warfare.* (Washington DC: Brookings Institution Press, 2000).

[73] O'Hanlon, 172.

attended to by, amongst others, the experimental organization NOBLE. Truly there are profits to be made by a more extended use of COTS, NATO off the Shelf (NOTS), Military off the Shelf (MOTS), Government off the Shelf (GOTS) and by improving older platforms, sensors, weapons and information systems instead of developing new ones. In addition, new asymmetric threats may also put different and even less costly demands on military materiel than on the old conventional battlefield. One of the cost driving factors in military innovation is the particular specification of the equipment related to endurance, hardship and redundancy. Although the prospect of such a battlefield is not entirely gone, much can be done with less advanced or less hardened equipment in, for instance, the war against terrorism or fighting insurgencies in an urban environment.

Another cost reducing idea is to exploit organizational networked experiences and technology from the private sector, or as Arquilla frames it: "We look to the business community for inspiration. Networked organizational forms are highly efficient, and we like to emulate that."[74] By tapping into the same hardware, software and expertise, R&D costs may be less and valuable time for experimentation saved. For instance, "In many cases, the same servers, satellites and fiber-optic networks, as well as software that major corporations routinely use, can be pressed into service to link images from Global Hawk unmanned aircraft with commanders and shooters on the ground." [75] Another example is the FBCB2[76] computer network technology that most recently has shown its usefulness in the Iraqi desert. Originally developed as a simple tool to keep track of truckers on America's highways, this satellite and radio-based tracking system has evolved into a highly advanced database and digital battle command system that identifies own users' location, friendly forces and other threats and obstacles. [77]

---

[74] John Arquilla in John Carey et.al, "Point, Click…Fire," *BusinessWeek online*, 7 April 2003. http://www.businessweek.com/index.html ((accesses 6 March 2004).

[75] John Carey et.al, "Point, Click…Fire", *BusinessWeek online*, 7 April 2003. http://www.businessweek.com/index.html (accesses 6 March 2004).

[76] Acronym for Force XXI Battle Command Brigade or Below

[77] William New, "Army Relying on New Battlefield Network Technology." Government *Executive Magazine*, Daily Briefing, 8 April 2003.

Similar approaches are possible in Norway if extensive cultivation of civilian – military cooperation takes place. In fact, in a small transparent country that also is dependent on high-tech industry, the opportunity to form a network of civilian businesses and the military to promote NCW innovations and procurements should be very good. Such cooperation has already started. A study of the initial Norwegian NCW system concept, including an ambition level, was worked out with three larger actors in Norwegian industry.[78] Furthermore, this group reviewed how the present organization, materiel, technology and competence could be exploited in an implementation phase and made several recommendations on necessary actions and how to proceed in the future. Parts of these conclusions are referred to in this thesis,[79] but the point here is to emphasize the importance of having the industry on board from the outset when new NCW technology and concepts are developed. This industrial cooperation should follow two converse principles. One the one hand, the military should seek strategic partnership with certain industrial corporations, particularly in areas where military demands require pure research and development of new ideas and innovations. On the other hand, the military should also economically exploit the diversity and competition in civilian industry and to a large extent, use COTS whenever possible to reduce unnecessary R&D costs.

O'Hanlon's second guideline is to "Redress existing military weaknesses and vulnerabilities. Doing so requires attention to a wide spectrum of subjects ranging from homeland defenses against missile attack and the terrorist threat to further improvements in U.S airlift and sealift." [80] These considerations are very much political questions and for Norway's part have been addressed when security policy and the importance of interests are discussed. In the next chapter, changes in the nature of war will be discussed as well, and together these changes should also influence future NCW capabilities. The main point is, nonetheless, that the funding needed to develop an adequate NCW capability in the future may only be found by narrowing the tasks of the Armed Forces to the essentials. At present, it may seem that the tasks are ill defined, not particularly

[78] The three industrial actors were: Teleplan, Ericsson and Thales. See Norwegian Chief of Defence. "Konsept for nettverksbasert anvendelse av militærmakt" *Forsvarssjefens Militærfaglige Utredning 2003.*

[79] See amongst others chapter 1 The Norwegian Approach to NCW.

[80] O'Hanlon, 172.

coordinated with other means of statecraft, and ranging over a general and far too large interest base.

Third is to "Sustain robust research, development, testing and evaluation (RDT&E) efforts, particularly in areas of basic research and development (R&D), as well as a joint-service simulation and experimentation." [81] These efforts apply to Norway as well, but as a small nation with a limited research environment, alliance and multinational cooperation will play an important part. Consequently, the Norwegian military transformation should be closely coordinated with NATO's transformation efforts and the NATO Council's Prague Capabilities Commitments (PCC).

A Norwegian contribution to these PCC initiatives is focused on establishing desired niche capacities within the Alliance. Focus on these capacities entails an increased role specialization and division of labor within the Alliance that will reduce the costs and need for resources. Moreover, identifying appropriate niche areas of specialization is considered a key to NATO's transformation.[82] The Norwegian approach to this demand is to focus on capabilities where the military already occupy high level competence and where these capabilities already meet national demands. Some of these capabilities are general in nature and inherent in most of the elements of the Norwegian force structure: for instance specialization in arctic warfare, expertise in littoral operations and mastering of demanding topography. Others nice capabilities are specially developed, amongst others through multinational operations, such as transport control, mine clearance, EOD elements, multinational logistic, special operations and intelligence. In an NCW perspective, Norway's approach makes sense. If the nations or their services are considered as nodes in a larger system, they cannot all develop and maintain the same capabilities. Networking the niche capacities will ensure that a multinational and joint task force can perform a larger range of tasks. In essence, this way of organization creates a larger result than the sum of connected entities. The prerequisite for the connection is interoperability and familiarity with the main body's (U.S.) operational concept.

---

[81] O'Hanlon, 172.

[82] Vice Adm Cebrowski cited in speech by Mr Robert G. Bell at the Norwegian International Defence Seminar on Technology, Counter-Terrorism and Future Force Structures in Lillestrom, Norway 14 Oct 2003. http://nids.ffi.no/proceedings/Bell/NIDS1-Bell-Future_of_NATO.pdf (accessed 23 March 2004).

Another initiative sees an increased need for multinational cooperation within the Alliance for development of technology, materiel, force capabilities, concepts and operations. Again, Norway sees the need to balance the transatlantic link against Europe. Instead of a spread focus, Norway tries to gather a few strategic partners concentrated around the North Sea basin in a North Sea strategy for multinational military collaboration. In addition to a shared geography, the five countries, the United Kingdom, Germany, Holland and Denmark also have a shared historical and cultural background that is anticipated to create less friction in a tighter military community. Examples of this strategy are the Norwegian-Danish-Dutch air force cooperation recently deployed in Kyrgyzstan, the Norwegian army's cooperation with the German-Dutch corps and the Navy and Special Forces' long standing relationship with the British. The strategy makes sense also in a strategic NCW perspective since it is almost impossible for a small node (Norway) to have the same strength of ties to all the nations or nodes in a large system such as NATO. By limiting the numbers of partners the hope is to build qualitatively better relationships and competence within this North Sea network that will give valuable and economic synergy effects. Furthermore, the strategy does not exclude other allies or partners in selective areas where such cooperation is necessary or mutually beneficial. In this regard Norway seeks to uphold the strong transatlantic link towards the U.S. with military cooperation on a broad scale.

O'Hanlons's last guideline is not to "pursue full-scale modernization with expensive next generation weapons platforms. Rather focus on making sure existing platforms remain safe and reliable. In addition, existing weaponry may be coupled with new information systems. In many cases, weaponry that that is already in the force today will be good enough for coming decades."[83] According to O'Hanlon, this point is the real bill payer for future innovations and procurement in the transformation process. Two historical examples that have provided a surprising superiority on the battlefield support his point.[84] The first is Germany's development in the interwar period where only a small number of transformed troops (10%), among a larger number of legacy forces (90%),

[83] O'Hanlon, 172

[84] Williamson Murray and Thomas O'Leary, "Military Transformation and Legacy Forces." *Joint Forces Quarterly*, Spring 2002.

created the necessary synergy to make a superior warfighting doctrine of combined arms – the Blitzkrieg. Similar were the U.S. experiences from the Gulf War, where a small and creative "think-tank" within General Schwarzkopf's staff was allowed to plan and execute a new and "unconventional" strategy utilizing an available, but very small portion of the force with stealth and precision guided munitions, to create confusion and disruption rather than the proposed systematic destruction of a roll-back strategy. Thus, the air defense system was neutralized, complete surprise was achieved, and the Iraqis never recovered from the initial psychological defeat. The key point is that a relatively small number of transformed forces can greatly improve the entire force. In this respect, innovative concepts, doctrinal and organizational development are more important than implementing new technology and weapons systems in the whole force structure. However, the latter is important as an enabler. Consequently, a radical transformation in the whole force may not be necessary, but the force still has to be receptive and adaptive to new concepts. Thus, the requirements for a cultural and mental change are crucial and perhaps the greatest challenge in the transformation process. Unlike the Germans in the interwar period, the same existential urgency to transform. is not felt in Norway.

The above is true for Norway's Armed Forces as well but there are limitations to this policy. In some key areas new procurements have already been deemed necessary. New frigates in the Navy are to be introduced in 2005. They will be supported by the NH90 helicopter package, which also includes new transport helicopters for the Army. Furthermore, both the Army and the Air Force are retaining a lot of their old platforms that need upgrading or replacements. Hence, expensive platforms such as new fighters, air transport and a new generation of mechanized vehicles are due in the not too distant future. Together these needs for basic investments put an enormous pressure on the expenses required to run daily activities and operations.

As a consequence, redirecting resources to fill the identified NCW gaps in the "info-structure," sensor components, decision components, effect components, data fusion systems, systems to create necessary situation awareness and systems for self-organizing, seems very difficult. In reality, Norway risks the danger that the number of entities in a network will be so small or fragmented that they will have little combat effect except when hooked up to a larger net, for example in NATO or a coalition of

forces. This problem was recognized in the earlier mentioned NCW study and one suggested solution is to replace volume for speed. Truly, superior speed has contributed to surprising victories throughout military history, as it did in the earlier mentioned Blitzkrieg concept against a larger number of allied troops actually prepared for a German attack. However, the advantage lasted only a while against an adaptive enemy that soon copied and obtained similar capabilities and reengaged in the battle with greater resources. The point is that sustainability and a wider range of capabilities to ensure flexibility will be needed in most conflicts or crises of certain duration. The lack thereof can easily be exploited by an adversary and mass speed will shortly outlive itself. Consequently, a NCW implementation must find the right balance between the range of capabilities, quantity and quality. Understanding and sensing the enemy is of less use if the means to touch him are not available.

The Norwegian NCW study also recognizes that calculation of any economic benefits of a NCW concept in its development or implementation phase should not be made.[85] Hence, it is difficult to see that investments in defense will not increase during this transformation process. Asking for money seems like an easy fix when a task within the given resources cannot be solved. In fact, at the beginning of the transformation process in the late nineties, a Norwegian general said he welcomed these economic restraints because it enforced necessary reductions in an obsolete organizational structure. Publicly, the armed force's have also been criticized for not delivering more fighting power for its 27 billion NOK annual allocation compared to, for instance, Sweden and Denmark that are similar sized countries. The general's statement and the critique might have been in order early in the transformation process when the goal of transforming the force in a NCW direction was less clear. Moreover, part of the critique stems from difficulties such as political friction, bureaucratic inertia, and cultural resistance of getting rid of a legacy that lasted almost 40 years. Many of these problems are now reduced and the bureaucratic mindset and military culture is more adjusted to a future reality of constant change.

[85] Norwegian Chief of Defence. *Konsept for nettverksbasert anvendelse av militærmakt*, 50.

However, the military is unlikely to conduct the transformation at the same economic thresholds that were maintained in the last decades of the Cold War. An analogy can be made to the business world. Few larger businesses and corporations believe that they can make more profit during the transformation process itself. On the contrary, the expected dividends come after, often a long time after, the investments. One example is the huge investments made in the development of the Norwegian oil and gas industry during the seventies. Perhaps this industry could serve as an example of how to enter the information age for the military. In the early seventies, the oil and gas venture was a national economic and industrial venture of large proportion for a small nation without prior off-shore drilling and production experience. Luckily the resources, competence or technology were not outsourced, but developed domestically and incrementally to the benefit of the people and the main land industry. Finally, after 20 years, large surpluses began to show in the state budgets and Norway is now one of the wealthiest nations in the world.

> Norway became a full-fledged oil nation in the mid-'70s. One of the main reasons for our success was that our shipping and related maritime businesses provided us with an administrative network and the technical and management skills needed to build up our oil industry. Through gains in efficiency, rationalisation, continuous adaptation to technological development and changed marketing, operating, as well as competition conditions on the continental shelf, Norwegian maritime industries not only managed to maintain, but also consolidate their positions." [86]

Now, there is a need to make an all-out effort for innovation and investment for society's and the military's entrance in the information age. For the military part, and contrary to the oil industry experience, the expenses will of course never create a surplus in the state budget but, both directly and indirectly, innovation could thrive, domestic civilian high tech industry could benefit and an overall enhanced security environment would also spill over to other sectors and society in general. In short, because the NCW implementation is so widespread in its doctrinal, organizational and technological scope, looking at red figures only in the defense budget, could be a very narrow-minded view of the whole society's benefit of implementing NCW.

---

[86] Helle Hammer, "The Norwegian shipping industry." Website about Norway by the Norwegian Ministry of Foreign Affairs. http://odin.dep.no/odin/engelsk/norway/economy/032001-990368/index-dok000-b-n-a.html (accessed 21 March 2004).

Arguably, this line of strategic thinking has been absent in Norway since the dependency on the NATO in 1947 and it goes along with not having an official national strategy that also encompass a military doctrine. This shift in attitude toward the military's role in society and defense spending will require immense political persuasion and a significant cultural change, but it could mean a rapid spiral transformation in a Norwegian context. Despite its size, Norway possesses both the resources and competence to implement NCW on a broad scale. It is first and foremost a matter of networking existing governmental agencies and private industry. The alternative of not choosing this path is incremental and evolutionary steps in the wake of the U.S.'s. and other larger strategic partners' NCW initiatives. Surely, the domestic competence and economic off spring from these initiatives will be less than if they were self-initiated.

E. THE CULTURAL RESISTANCE OF EXPLOITING "SOFT POWER"

Previously, it has been argued that a new mindset is required for thinking about security policies, national interests, technology, and perhaps also the economic approaches when implementing NCW. Furthermore, that a tighter integration between the military and civilian society is necessary to reach the ambitious goals depicted in the tenets of NCW, and that tighter interagency networking will require a significant cultural change amongst Norway's political and military establishments. This cultural change is necessary in other areas as well if the NCW implementation is to be successful. First and foremost is the way of approaching the tenets of IS as a foundation for NCW. In Chapter Two the importance of IS to achieve full spectrum dominance was emphasized. Implied in this is that information must be consciously exploited at all levels of warfare and that there is a network that timely connects and communicates vital pieces of information between the intelligence community, key actors and decision makers. "Information is the lifeblood of Information Age organizations. Information-related policies and architectures define the topology and determine the capabilities of an organization to distribute this vital resource."[87]

Unfortunately, in the Norwegian military, or in the government or bureaucracy in general, there is very little tradition to purposefully exploit the soft power of information.

[87] Alberts and Hayes, *Power to the Edge,* 186.

Organizational structures for the conduct of IO have only partially been developed and then mostly at the operational and tactical level with emphasis on EW, OPSEC and Physical Destruction. The non-technical capabilities of IO such as deception and PSYOPS are given very little attention and are practically not developed at all. Nor have IO related activities such as public affairs and civil affairs had any prominent place in the planning or conduct of military operations. The absence of IO efforts is also reflected in the emerging Norwegian NCW literature. In the first published introduction to NCW, the reader is in fact cautioned not to make a tight link between IO and NCW even if a direct relationship were indeed recognized. The primary point of intersection between the two was seen within IA and OPSEC.[88] In the new NCW concept, IO as an enabling concept is mentioned directly only once, and then in a general context on how to achieve IS.[89] Furthermore, the proposed IO ambition in the next planning period is limited to enhance the PSYOPS and EW capabilities and to establish a CNO capability. In addition, the command structure at the strategic and operational level should have the ability to lead and coordinate *military* information operations, but the organizational consequences of such a capability is not mentioned.[90] The IO relationship to the political level is not mentioned in the study, which additionally support the impression that it is mainly tactically focused. Thus, it is reasonable to conclude that IO is not yet functioning as a strategic instrument nor yet seen as an enabler shaping the operational environment and creating the foundation for IS in the Norwegian Armed Forces. In a larger perspective this confirms the impression, also shared by Alberts and Hayes, that "… most military organizations continue to see Information Operations as a separate function that is managed outside the traditional operations organization".[91] It could be argued that the situation in the Norwegian military is even worse, because there are no dedicated entities outside the traditional organization that have the resources, competence or skills needed to conduct strategic or operational IO on a broader basis. Emphasis continues to be made on information management and the technical information structure within the

88 Norwegian Staff College, "Introduksjon til Nettverksbasert Forsvar", *Militærteoretisk skriftserie* - nr 1 2001, 9.

89 Norwegian Chief of Defense, *Konsept for nettverksbasert anvendelse av militærmakt*, 28.

90 Norwegian Chief of Defense, *Forsvarssjefens Militærfaglige Utredning 2003,* 13.

91 Alberts and Hayes, *Power to the Edge,* 58.

conventional establishment. Overemphasizing the tactical and technical side of IO will be at the expense of more important issues in the cognitive domain such as how to influence a larger part of a population or an adversary's key decision makers.

It is difficult to explain this lack of interest in information as power or a tool of influence, but the phenomena is also reflected in other areas of Norwegian governance. One explanation can be that IO is seen as an unfair method using non-desirable political and military means. Obviously IO is surrounded by myths especially created through the PSYOPS and Deception elements where secrecy, lies and indirect methods are some of the main ingredients for success. Perhaps aspects of IO contradict the Western perception of the warrior ethos where honor, bravery and fairness on the battlefield have been admired since ancient times. We complement the Viking duels on the beaches; the Knights conduct of honor during the Middle Ages; the organized and civil battles of the American Civil War; the daring commando raids against superior defenders during WW II; and lastly, modern Special Forces' remarkable successes in difficult takedowns of embassies, airliners and other objects. We tend to forget that the Vikings' successes also were information dependent on their reputation created by merciless atrocities; that mayhem and treachery also were the trademark of royals, knights and the priesthood during the crusades; that Sherman purposely created fear through his campaign against the civil population in the South; that the commando raids often were heavily dependent on supporting deception plans; and that recent Special Forces' successes have often depended on a deliberate breakdown in the established trust that is achieved through negotiations. Hence, throughout history Western nations have relied more on elements of IO for successes in warfare than not.

Also part of the problem to fully recognize IO as a legitimate tool of warfare is the fear from our own population that they themselves may be exploited or deceived. In fact, when describing the proposed IO efforts in the defense study, the Norwegian Chief of Defense carefully reassures that IO is not directed against its own or allied populations. No other warfare concept or weapon system needs such an introduction. This visualizes the more troublesome aspects of IO and the political skepticism to embrace it. Certain elements of IO are not easily seen as viable and legitimate means of pursuing political objectives. Terms, such as political warfare and propaganda remind us

of totalitarian regimes' efficient use of these means to suppress their own populations and influence their opponents. The Third Reich's propaganda machinery and the Soviet Union's excessive use of psychological operations stand out as examples in this regard.

Nevertheless, IO is recognized as an instrument that can reduce the costs of warfare in more than an economic sense. In addition, other countries and future potential adversaries to the Western Alliance are acknowledging IO as an increasingly more important tool of modern warfare. Today's Russia continues to develop its IO capabilities based on in-depth expertise from the communist era. Amongst others is an active IO R&D program, attempts to create computer viruses as weapons, and institutionalized efforts of IO such as the creation of the Federal Agency for Government Communications and Information.[92] Correspondingly is the Chinese emphasis on IO efforts as a prominent feature of future wars. Major General Wang Pufeng, former director of the strategy department states that: "In the near future, information warfare will control the form and future of war. We recognize this developmental trend of information warfare and see it as a driving force in the modernization of China's military and combat readiness."[93] These contrasting views of IO are striking and an inferred conclusion may be that the Norwegian perception of the legitimacy and political and military usefulness of IO is indeed limited.

The aversion to fully exploit the psychological means of statecraft is also present in the U.S., perhaps the Western country, apart from Great Britain, that has gone the furthest to develop and exploit the soft power of information, including public diplomacy and IO. According to Dan Kuehl, professor at the National Defense University in Virginia, one indicator of IO's reduced significance in the Bush administration is that the new U.S. national strategy has only one reference to IO, which, "is a step backwards from its predecessor."[94] Furthermore, Kuehl states: "What you are seeing there is perhaps the reaction to September 11. What's missing, in my opinion, is a sense of the power and synergy of information as an element of national power, and I hope this omission is

[92] Carla Bass, "Building Castles on Sand", (Air War College: Maxwell Paper No.15, 1998), 16.

[93] Sited in Carla Bass, "Building Castles on Sand" , 23

[94]Dan Kuehl, Interview with Wanja Eric Naef about Information Operations, London, July 2003. Infocon Magazine Issue One, October 2003. http://www.iwar.org.uk/infocon/print/io-kuehl.htm (accessed 22 March 2004).

rectified in the next such National Security Strategy." One impact of loosening this important notion of the "war of ideas" through IO can perhaps be seen in Iraq. While the conventional battles were convincingly won, the U.S. has so far not been particularly successful in winning the war of ideas in the Iraqi population or elsewhere in the Middle East.

The war of ideas is undoubtedly important but it must also be supported by a country's own population, at least in a democracy, to be viewed as legitimate. "A democratic people – or the influential portion that cares what the nation does in international politics – associates itself morally and emotionally with national policies and actions, and demands that the government reflect its sentiments."[95] Thus, IO at the strategic level can be conflicting because there is a perception that it is about diverging ideas and opinions. Arguably, the "power of the people" has also increased in the information age. New technology and forms of communication have made it easier to participate in political debates. As a consequence, "The new social forms of the early twenty-first century will greatly enhance the power of social networks."[96] This may have an important impact for IO in the future. In addition, because of the variety of means available for expression and communication it can also be difficult to get a grasp of what the "people's opinion really is."

On the other hand, Carnes Lord warns us about the tendency to focus on strategic IO only as a conflict of ideas, ideologies and opinions. In fact, under many circumstances this perception could be seriously misleading. "Psychological and political warfare is also about cultural and political symbols, about perceptions and emotions, about the behavior of individuals and groups under stress, about the cohesion of organizations and alliances."[97] This point is extremely important to stress for the GWOT and in the current post-conflict phase in Iraq. Obviously there is an ongoing war of ideas in these matters that requires attention; but, it might be more important to emphasize the elements of

---

[95] Robert Osgood, *Limited War: The Challenge to American Strategy* (Chicago: The University of Chicago Press, 1957), 28.

[96] Howard Rheingold, *Smart Mobs: The Next Social Revolution* (Cambridge: Perseus Publishing, 2003), xviii.

[97] Carnes Lord, P*olitical Warfare and Psychological Operations* (Washington: National Defense University Press, 1989), 17.

strategic IO that Lord refers to rather than the stigmatizing larger ideological and religious differences between Western and Islamic countries.

Additionally, there is a misconception that psychological-political operations should be entirely directed against an opponent. It is equally important to bolster a countrys' policies and military operations through information operations. Thus, highly important target audiences for this influence could also be neutral, allied or semi-allied nations, depending on the adversary's objectives.[98] The manner in which this can be done is a matter of ethics and institutionalized rules of conduct and need not be contradicting to democratic values. On the contrary, openness and promoting the truth from a Western perspective should be the key issue, but one need amongst others the psychological skills and the tools of propaganda to influence the target audience efficiently.

In this view, the Norwegian approach to achieve IS seems incomplete without properly emphasizing the cognitive domain in a NCW implementation. Moreover, the development of the necessary psychological means and IO capabilities will have to reach far outside the military. It must be recognized as a legitimate part of future warfare by the political establishment and interagency effort and cooperation is necessary to succeed. Without these efforts in the cognitive domain, the anticipated benefits and efficiency of NCW will only be partly fulfilled. David Potts speaks of this necessary shift in culture of viewing psychological operations in the following:[99]

> Deploying decision against other such forces in a defined battlespace, is giving way to deploying forces to create the conditions in which a decision might be achieved outside the military domain. The military line of operation in a campaign is therefore not just one of a number of lines of operation, it is subordinate to and constrained by others: diplomatic, political and economic and increasingly by Information Operations, directed from the highest political level, and legal considerations.

As a consequence, a Norwegian NCW concept should give IO far more attention in an implementation phase. Emphasis on this side of the information structure could also be a cost reducing factor as IO efforts will contribute to identify and prioritize the

---

[98] Lord, 17.

[99] David Potts, *The Big Issue: Command and Combat in The Information Age* CCRP Information Age Transformation Series, February 2003, 315 (Reprint from Strategic and Combat Studies Institute Occasional Paper Number 45, March 2002).

technical side of the structure. According to Kuehl, IO must be seen as a process and an enabler to synchronize, synergize and deconflict activities across the interagency spectrum. IO is a "source multiplier," and not a separate weapon capability. It is a "strategy, a campaign, and a process that is supported by traditionally military forces."[100]

F. THE ROLE OF PUBLIC DIPLOMACY

A key aspect of soft power can be found in the area of public diplomacy. Much of the same resistance and attitudes as described in an IO context can be observed within this tool of statecraft as well; but, first public diplomacy needs to be clarified. Starting with some definitions, public diplomacy is:[101]

> Public diplomacy differs from traditional diplomacy in that it involves interaction not only with governments but primarily with nongovernmental individuals and organisations. Furthermore public diplomacy activities often present many differing views represented by private American individuals and organizations in addition to official government views. (Edward Murrow, 1963, speaking as director of USIA)
>
> Public Diplomacy seeks to promote the national interest of the United States through understanding, informing and influencing foreign audiences. (Planning group integrating USIA into the Dept. of State, 20 June 1997)
>
> The purpose of public diplomacy is to influence opinion in target countries to make it easier for the British Government, British companies or other British organisations to achieve their aims. The overall image of Britain in the country concerned is of great importance – but this is not to say that it is the only factor. The most important factor will usually be the actual policies of the British Government and the terms in which they are announced and explained by Ministers. In most countries a broadly internationalist posture will be positive. A narrow and open pursuit of national interests at the expense of others will be negative. For example, the Government's handling of the beef crisis in the summer of 1996 had a negative effect not only on Britain's ability to get its way on other EU issues, but also on the view taken of Britain in many non-EU countries. (Sir Michael Butler, former British representative to the EU, 2002)

Furthermore, in a U.S. context, Carnes Lord describes public diplomacy as a key strategic instrument for shaping and communicating fundamental political and

[100] Dan Kuehl, 6

[101] Definitions in Mark Leonard, *Public Diplomacy* (London: The Foreign Policy Centre, 2002), 1

ideological ideas in order to affect a foreign audience. It may consist of elements such as international information programs, for example voice of America; educational and cultural programs, such as educational exchange; political action and public affairs.[102] Clearly, the military has a role to play in public diplomacy as well, firstly, in a supporting role where the armed forces' broad international engagement directly or indirectly could be exploited to promote the government's official interests and images. Secondly, in a supported role for the government to explain the basis for having a certain military structure, the need for a military transformation into the information age, and also the need to use military power under certain conditions. The latter will be of particular importance in the future in light of the recently disputed interventions in Afghanistan and Iraq.

The Norwegian government has begun to recognize public diplomacy as an important tool to enhance Norway's image in the world, but, so far, the military's role is very moderate and perhaps even contradicting of the desired image that Norway wants to portray of itself. In a report on Norwegian Public Diplomacy, compiled by the British research body The Foreign Policy Centre in cooperation with the Norwegian Foreign Ministry, it is acknowledged that Norway faces the problem of invisibility in the world society.[103] A number of factors contribute to the invisibility:[104]

- it is small in population, economy and presence;
- it is isolated politically, geographically and culturally;
- it lacks linguistic attraction, many Norwegians speak English but not vice versa;
- it lacks brands or icons , there are no emissaries for the Norwegian identity;
- it is similar to Scandinavia – its shared culture does not help to distinguish it from the rest.

Arguably, that the rest of the world knows little about the Norwegians is a competitive disadvantage within most sectors. Thus, the need for a public diplomacy

[102] Carnes Lord, "The Past and Future of Public Diplomacy"*, Orbis 42 (1),*1998, *49-73.*

[103] Mark Leonard and Andrew Small, *Norwegian Public Diplomacy* (The Foreign Policy Centre, June 2003), 1. Norwegian Ministry of Foreign Affairs http://odin.dep.no/archive/udvedlegg/01/06/ml10_018.pdf (accessed 22 March 2004).

[104] Mark Leonard and Andrew Small, 2.

strategy arises. This thesis will not elaborate Leonard's and Small's distinguished strategy, but of particular interest is the suggestion to strengthen Norway's image based on four desired perceptions: [105]

- *Humanitarian superpower*, emphasizing Norway's contributions to aid, its role in peace-keeping and peace processes and its commitment to developing new kinds of global governance.
- *Living with nature*, emphasizing Norwegians' unique relationship with nature, exploiting its potential whilst pioneering ways of protecting the environment.
- *Equality*, emphasizing the value of equality which is deeply embedded in Norwegian culture and Norway is living proof that equality and economic dynamism can be combined.
- *Internationalist / Spirit of adventure,* emphasizing Norway's history which is literally sprinkled with famous adventurers whose endeavors are only partially known – from the Vikings and Heyerdahl's Kontiki to Amundsen's polar quests and the modern BASE jumpers to sport performances.

Although interagency efforts are stressed to develop and implement a public diplomacy strategy, the Norwegian Military role in such a strategy is only mentioned vaguely despite its contribution to all of these images. Obviously, the first one is relying extensively on military contributions. Actively using the Coast Guard and Navy to protect and ensure a healthy environment in Norwegian waters is an example of the military contribution to the second image. The third image is a cornerstone value in which the military's basis for existence is found. Lastly, in the internationalist / spirit of adventure image, the military's role has also been important. The military's contribution to Norwegian polar history and its role in organizing the 1994 Winter Olympics are some examples. The point here is not to exaggerate the military's role in public diplomacy, but

105 Mark Leonard and Andrew Small, 3. This is not official Norwegian policy. The state secretary Thorhil Widvey underlined in a speech in Ottawa 7 Nov 2003 that "these stories are in no way politically agreed upon as the stories to tell the world. For instance, the term "humanitarian superpower" has met some well-founded opposition on the basis that it expresses a superiority with which we do not wish to be associated. Personally, I also think that trade and industry disappear somewhat in these formulations. However, they constitute a point of departure from which to continue working" http://odin.dep.no/ud/norsk/aktuelt/taler/taler_politisk_ledelse/032171-090183/index-dok000-b-n-a.html

by not including the military efforts opportunities for public diplomacy are missed. Thus, introducing NCW in the future should also imply to "net" and make visible the military role in a broader society. It should also bolster military operations and activities.

In the infancy of the Norwegian Foreign Ministry's attempt to create a public diplomacy strategy, the military's role is very unclear. For instance is the issue of peace keeping operations, the following citation from the report shows how this image should be portrayed: [106]

> The first aspect is about Norwegians as engaged global citizens: peacemakers and peacekeepers – the blue helmet rather than the white dove; thinkers and practitioners at the forefront of debates about soft power with a sophisticated understanding of global security. In order to avoid both undermining its role in peace negotiations and provoking other partners, emphasis needs to be placed on the right aspects of the message – Norway as a partner, facilitator and good multilateralist – and attention should only be drawn to peace processes once they are firmly established.

Without a broader contextual description of the military's role in society and the current military engagements abroad, this portrayed image of the Norwegian governments use of military power could be misleading and interpreted just as much as an annoyance to official foreign policy goals. The Norwegian government's willingness to use military power for other purposes related to the country's self interests should be portrayed as well. Although important, the use of military power should not be hidden by the humanitarian aspect only. As a consequence, it is important to coordinate Norwegian security and defense policies more closely in public diplomacy efforts. An NCW implementation process should coordinate these efforts as well and establish an adequate political – military network to ensure that military interests are attended to and do not conflict with any public diplomacy strategy.

[106] Mark Leonard and Andrew Small, 3

G. CONCLUSION

This chapter has elaborated some of the important factors in the Norwegian strategic environment that should be factored into a NCW implementation process. There are several others that are not mentioned. Not because they are not important, but because they are less distinctive in a NCW concept compared to other warfighting concepts. Factors such as Norway's topography and demography, the distinctiveness of the political system and the country's economic and industrial strength will have to be taken into account in any warfighting concept. Hence, they will not be discussed separately and in detail here. Likewise, some other factors, such as the social structure, society's and the military's adaptability to new technology, past war experiences and the populations motivation or will to fight will be commented on later in relation to the changes in the nature of conflict, or to the transformation of war, as Martin Van Creveld named his ground-breaking reinterpretation of armed conflict in 1991.

Conclusively, this chapter's goal was to make a distinction on factors in the strategic environment that perhaps require a different approach to how the concept. of NCW should be implemented. Norway's strategic freedom of maneuver within the power triangle between Russia, the EU and the U.S. is one such determining factor. Norway's closeness to Russia, its non-membership in EU, and attempts to balance the transatlantic link combined with the general global security policy developments, suggest that Norway must develop a broader range of capabilities in order to conduct independent crisis management. An alternative approach, where Norway, for instance, became a full partner of the EU, could perhaps change the formula, but that is not the current assumption. Moreover, the independent NCW capabilities should be tailored specifically to meet Norway's geopolitical situation, including the potential conflict portfolio that comes with Russia as a neighbor.

The NCW capabilities should also be tailored to fit Norway's specific interests that there is a political will to defend by military means. These interests need to be further defined. In the example used to illuminate this issue, many of these are maritime interests. This implies that an intra-agency and intra-service network at all levels within the maritime sector should be developed and maintained not only in times of crisis but also on a daily basis.

NATO continues to be the cornerstone in Norwegian security and the NATO transformation process and NCW development should be closely followed. In this regard, Norway is well ahead with several initiatives pursuant to the PCC requirements. However, when developing NCW capabilities, Norway should be critical of implementing blue prints from the larger partner nations. Norway's distinctiveness, with a smaller power base and other natural conditions, may demand a different military doctrine and other technological solutions. In addition, Norway should be prepared to raise its own interests with more force as the NATO network becomes more politicized in a more globalized and interest based world.

The economic and technological aspects of a NCW implementation invite new ways of strategic thinking. The assumptions of NCW as an expensive warfighting method in the information age can be proven wrong if other strategic, conceptual, and doctrinal sides of the implementation are prioritized, rather than focusing on expensive high quality materiel throughout the whole military organization. However, because of heritage and a considerable gap in the predicted NCW structure, it is unlikely that total defense spending can be reduced in the short future. On the contrary, it is likely to increase; but if a long-term view is taken, and NCW is implemented in an orderly fashion and in cooperation with Norwegian industry, the implementation may also give good returns to both civil and military society.

The Norwegian culture and attitude to the significance and efficiency of soft power, and in particular IO and public diplomacy, may be a serious obstacle to the achievement of information superiority. Understanding and exploiting these tools could be a cost efficient means to enhance daily operations and combat efficiency, in addition to the other humanitarian costs that inevitably are connected to war. The expected dividend of NCW most likely can never be collected until a grasp of the prospects and limitations of IO and public diplomacy within a Norwegian context is achieved.

.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CHANGES IN THE NATURE OF CONFLICT

The prospects for NCW as an information-enabled warfighting concept and certain aspects of Norway's strategic environment that should influence a NCW implementation strategy have been discussed previously. Attention is now turned to the nature of conflict where questions such as, is the war high-tech or low-tech, short or long, limited or unlimited, conventional or unconventional, become important to determine the impact of the information age on future forms of warfare. An NCW concept must aim to embrace all these characteristics to a larger or lesser degree according to their relevance. Surely, each conflict is unique as Clauswitz proposed, but there are perhaps some general lessons learned from the characteristic features of the information age and a more thorough analysis of future adversaries that will help determine the mission challenges, opportunities and constraints in the future. Hence, the latter elements will be the focus of this chapter. As depicted in the model below,[107] which further breaks down the elements in Figure 1, an analysis of these factors should contribute to identifying the specifics of a NCW concept as guidelines in an implementation strategy.

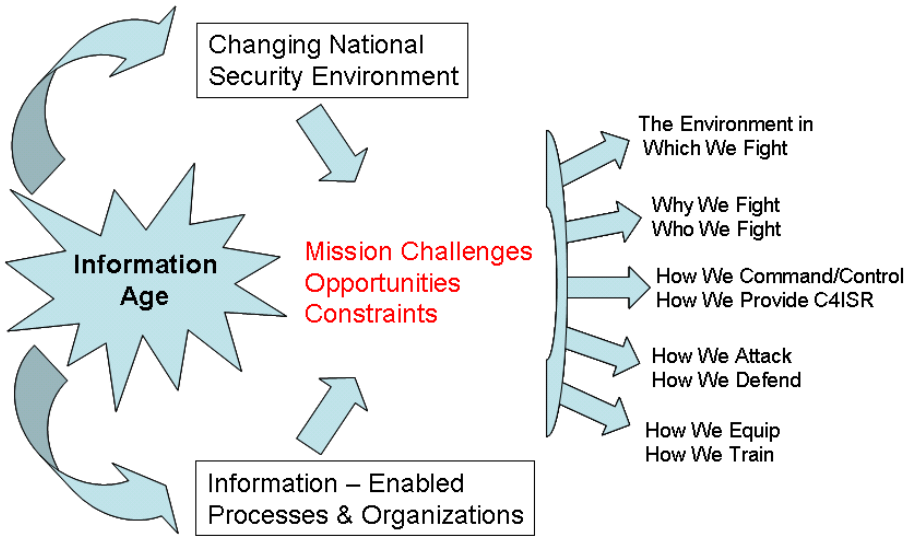

Figure 8. The Environment (From Alberts, 2002)

[107] Model adapted from Alberts, *Information Age Transformation: Getting to a 21st Century Military* (CCRP Publication Series, June 2002), 34.

With regard to the consequences for a Norwegian implementation strategy the findings in this chapter will be more general in nature and they will have a broader application. They should, nevertheless, have a prominent place when a NCW strategy is mapped out.

A. NOTES ON THE REVOLUTION IN MILITARY AFFAIRS

Since the end of the Cold War, it is apparent that the "nature of war" in general has changed. Total nuclear war and large conventional clashes between NATO and Warsaw Pact forces on the battlefields of Europe now seem distant and military doctrines based on attrition warfare have become antiquated. Or at least so it seems. Since the early nineties, sophisticated armed forces around the world have adopted a maneuver-oriented doctrine and are in a state of constant transformation towards even more flexible and joint force capabilities. The contemporary revolution in military affairs, primarily based on technological progresses is believed to further and fundamentally change future forms of war. In essence, changes will take place in three general classes of warfighting activities:[108]

- In the perfection of traditional combat
- In the evolution of nontraditional missions such as special operations, humanitarian assistance, counter-drug operations, peace operations and counter-proliferation
- In a new form of war unique to the Information Age focusing mostly on Cyberspace and the information domain

However, it is debatable if the current information revolution will have such an impact. According to Richard O. Hundley, who has investigated military technology and military revolutions in the 20th century, the following defining characteristics must occur in a true RMA:[109]

"An RMA involves a paradigm shift in the nature and conduct of military operations;

---

[108] Alberts, *Information Age Transformation*, 39.

[109] Richard O. Hundley, "Past Revolutions, Future Transformations", (Santa Monica: Rand, 1999), 9.

- which either renders obsolete or irrelevant one or more core competencies of a dominant player,
- or creates one or more new core competencies, in some new dimension of warfare,
- or both."

By his definition Hundley argues that, primarily because of lack of empirical or historical evidence, it is premature to characterize the current military technological, doctrinal and organizational development as an RMA. It is simply too soon to tell: but, a revolution is perhaps emerging or has the potential to become one.[110] The point here is not to engage in a theoretical discussion about whether a RMA is occurring or not, even if the discussion is highly relevant since the belief that it is, in fact happening, is drawing a large amount of resources to its attention. More important, are perhaps Hundley's findings of other characteristics showing that RMA is more than new technology. Some of his results based on the same historical examples are:[111]

- RMAs are rarely brought about by dominant players.
- RMAs frequently bestow an enormous and immediate military advantage on the first nation to exploit them in combat.
- RMAs are often adopted and fully exploited first by someone other than the nation inventing the new technology.
- RMAs are not always technology-driven.
- Technology-driven RMAs are usually brought about by combinations of technologies, rather than individual technologies.
- Not all technology-driven RMAs involve weapons.
- All successful technology-driven RMAs appear to have three components: technology, doctrine, and organization.
- There are probably as many "failed" RMAs as successful RMAs.
- RMAs often take a long time to come to fruition.
- The military utility of an RMA is frequently controversial and in doubt up until the moment it is proven in battle.

Acknowledging these points should lead to the investigation of other aspects of the contemporary RMA before implementing a NCW strategy. Perhaps focus

[110] Hundley, 19

[111] Hundley, 11-17

should be more on adversaries' strategies or preferred tactics while simultaneously exploiting the advantages of new information technology. Losing focus on enemies might prove disastrous when the NCW concept is put to the ultimate test on the battlefield. The actual RMA may instead be determined by the adversaries in what tends to be called asymmetric warfare. Means such as guerrilla and terrorism tactics targeting vulnerable aspects of society such as, densely populated areas, transport and communications, power supplies and environmental high risk facilities can be highly effective in modern societies. These strategies and tactics may render net-centric forces, advanced information and weapons systems more or less useless if these capabilities are allowed to be developed within a conventional and military framework only. This discussion is part of what many scholars have labeled a counter-revolution, a second revolution that includes countermeasures that obviously seek to outmaneuver the comparative advantages coming from a technology driven RMA.[112] Again, the key point is not semantics regarding RMAs, but to constantly use creativity and stamina in a thorough analysis of potential adversaries' activities and responses in accordance with the lower left side of Figure 1. For sure, as the September 11 disaster and the most recent terror attacks in Madrid have shown, the enemy obviously never rests and new technologies will never make the "fog of war" so transparent in the future to fully prevent similar incidents.

Contributing to further defining the characteristics of an RMA, Eliot A. Cohen has identified four key questions that need to be answered to understand the implications:[113]

- Will the revolution change the appearance of combat?
- Will it change the structures of armies?
- Will it lead to the rise of new military elites?
- Will it alter countries power position?

---

[112] For elaboration on the second revolution see amongst others James Stavridis, "The Second Revolution", *JFQ,* Spring 1997,

[113] Eliot A. Cohen, "A Revolution in Warfare", *Foreign Affairs*, Volume 75 No. 2, March/April 1996, 43-44.

The answer to these questions may identify important mission challenges, opportunities and constraints that can provide guidelines on what to emphasize in information-age warfare.

Cohen's qualified answer to the first two questions is in many respects reflected in Chapter II in the discussion of the prospects of NCW, IS and in new ways of organizing or networking the force. In addition this chapter also highlights the opportunities an NCW concept represents for future warfare. Concepts such as knowledge-based warfare, information warfare, shock warfare, swarming and netwar are pertinent labeled concepts that give an idea of the development of information age warfare. In addition, Cohen addresses a few other points. One is that an increased incentive for preemption may grow due to the domination of long-range intelligent precision weapons.[114] Combined with a belief in a counterrevolution, the first blow can indeed prove to be decisive in future conflicts. The recent intervention in Iraq may serve as an example of the U.S. and the Coalition institutionalizing this principle. Part of the preemption formula is also the fear that WMD may be used by non-state actors or rogue states. In this respect, with the convergence between new technologies and new terrorism, preemption and/or prevention by democracies to confront intolerable regimes, may be seen as both necessary and courageous.[115] Cohen also highlights an increased use of covert means, for instance in cyberspace, as another side of the preemption strategy. "Such attacks – to which an information-dependent society like the United States is particular vulnerable – could have many purposes: blinding, intimidating, diverting, or simply confusing an opponent", however, "How such wars initiated by information strikes would play themselves out is a matter of tremendous uncertainty.[116] Some aspects of this uncertainty will be addressed later in a discussion of some of the constraints in the concept of information superiority.

In his third question, addressing the structure of military organizations, Cohen tentatively describes militaries of the next century. Among other factors, it will rest on

---

[114] Cohen, 45.

[115] William Shawcross, *Allies: The U.S., Britain, Europe and the War in Iraq,* (New York: PublicAffairs, 2004), 233

[116] Cohen, 46.

long voluntary service, be increasingly joint, and have more "quasi services" operating, such as Special Forces and information warfare entities. Also, the use of supporting civilian contractors on the logistical and analytical side will increase. Cohen also points out that "The radical revision of these structures will be the last manifestation of a revolution in military affairs, and the most difficult to implement" [117].

Lastly, Cohen addresses the changing power of states. The United States' position as the sole superpower is probably uncontestable and it is perhaps the only country that can exploit the revolution to its fullest. However, other powers have great ambitions as well. China is emerging as perhaps the greatest challenger to U.S. global influence while Russia, as mentioned before, is reemerging as a power that seeks both regional and global power. Moreover, the contemporary revolution "offers tremendous opportunities to countries that can afford to acquire expensive modern weaponry and the skills to use it properly."[118] In this respect, size matters less and Cohen points to Israel, Taiwan, Singapore and Australia as examples of countries that can do more against larger opponents than was ever before imaginable.[119] In the information age, a large population and industrial capacity means less than in the past and the ability to translate organizational, economic and technological power into military capabilities can significantly alter a regional or local military balance. This could be true also for a small country like Norway. As a modern, high-tech oriented and wealthy nation, Norway's willingness to balance the risk of transforming its military into networked modern information age forces can yield great benefits in the sense of increased influence and security.

B. ORGANIZATIONAL CHALLENGES AND CONSTRAINTS

According to some scholars, the key challenges for transforming Western militaries lies not in the technological challenges ahead, but more on the doctrinal and organizational changes that must come. These changes are emerging either as a result of the opportunities posed by developments in the information age or as constraints by the

[117] Cohen, 48.

[118] Ibid. , 50.

[119] Ibid.

very same. It will go too far here to expand on all the types of organizations or organization principles that are envisioned for militaries in the information age, but in general two organizational doctrines, as proposed by Arquilla and Ronfeldt, seem particularly fit for networked actors.[120] One is to organize in a seemingly "leaderless" way. Multiple leadership with consultative and consensus-building mechanisms for decision making are some of the organizing principles. The edge organization described in Chapter II, with the empowerment of individuals at the edge of an organization is a major doctrinal step in a less hierarchical and leader-independent direction. Moreover, the power to the edge concept is considered to be a necessary condition for networked force to reach self-synchronizing capabilities.

The second proposed organizational doctrine is "swarming." According to Arquilla and Ronfeldt, swarming can be viewed as the idea of "engaging an adversary from all directions simultaneously, either with fire or in force."[121] However, swarming is more than a tactical concept. Coupled with information age technologies, IO and the emergence of well informed and lethal small units such as Special Forces, it may be regarded as a mode of conflict having a fundamental impact on doctrine development. In addition, a study of swarming in nature, swarming-techniques during past military conflicts, and contemporary organizations' use of swarming-techniques, in cyberspace for instance, have proven that swarming concepts can be highly effective.[122] Thus, there is an opportunity for modern militaries to exploit this efficiency in NCW where the infrastructure to wire decision makers, sensors and shooters already is in place. Moreover, in a technology driven RMA, swarming is an opportunity to "give network-centric concepts operational life through organizational and doctrinal innovation."[123] Since the notion of swarming is relatively new in modern military terms, some further definitions of swarming are useful to understand different variations of the concept.

---

[120] Arquilla and Ronfeldt, *Networks and Netwars*, 333.

[121] John Arquilla and David Ronfeldt, *Swarming & The Future of Conflict* (Santa Monica: Rand, 2000), vii

[122] Arquilla and Ronfeldt *Swarming & The Future of Conflict*, 1-3.

[123] John Arquilla and David Ronfeldt, "Swarming: The Next Face of Battle", *Aviation Week & Space Technology,* September 29, 2003, 66.

Below are some that were presented at the Joint C4ISR Decision Support Center conference on swarming in network enabled C4ISR 13-14 January 2003:[124]

> Swarming … is a deliberately structured, coordinated, strategic way to strike from all directions, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions. It will work best – perhaps it will only work – if it is designed mainly around the deployment of myriad, small dispersed, networked maneuver units.[125]
>
> A swarming case is any historical example in which the scheme of maneuver involves the convergent attack of five (or more) emiautonomous (or autonomous) units on a targeted force in some particular place. "Convergent" implies an attack from most of the points on the compass.[126]
>
> A collection of autonomous (or semi-autonomous) entities which rely on local sensing and simple behaviors – interacting in a way that a more complex behavior emerges from entity interactions.[127]
>
> A smart mob[128]
>
> [In] smart mobs … leaders may determine an overall goal, but the actual execution is created on the fly by participants at the lowest possible level who are constantly innovating, [Howard] Rheingold notes. They respond to changing situations without requesting or needing permission. In some cases, even the goal is determined collaboratively and non-hierarchically.[129]

A doctrine that includes swarming concepts represents a number of challenges regarding command and control and organizational aspects. With regard to C2 some of the challenges are that the characteristics include:[130]

– Diverse information functions, entities.

---

124 Definitions from Joint C4ISR Decision Support Center: Conference Proceedings, 13-14 January 2003 *Swarming: Network Enabled C4ISR* http://www.iwar.org.uk/rma/ (accessed 28 April 2004).

125 Originally in Arquilla and Ronfeldt (2002), vii

126 Originally in Sean J. A. Edwards, *Swarming on the Batttlefield; Past, Present, and Future*. p. 2

127 Originally in B. Clough, UAV Swarming? *So What Are Those Swarms, What Are the Implications, and How Do We Handle Them?* p. 3.

128 Howard Rheingold

129 Originally in Joel Garreau: *Cell Biology: Like the Bee, This Evolving Species Buzzes and Swarms*, Washington Post, July 31, 2002, p. C01

130 C. Defranco, F. Escobar, R. O'Connell, Parunak, et al. in John Hopkins (Physic Laboratory, 4-7 November 2002) in Joint C4ISR Decision Support Center: Conference Proceedings

- Distributed computation to reduce communications bandwidth.
- Decentralized control to avoid vulnerability and bottlenecks.
- Dynamic adaptability to changing battlespace.

These characteristics are to a certain extent incorporated in today's operational principles based on a maneuver-oriented doctrine; but the swarming requirements for shared situation awareness, autonomy, self-organization and simplicity go much further. Adding up, are the organizational requirements of distributed or dispersed forces and a sufficient presence of a large number of forces. The latter clearly represents a challenge for smaller nations, but numbers can be reduced if the forces have the necessary information advantage, for instance, based on detailed local knowledge of the battle space, and if organized in an efficient size.

Moreover, for Norway's case, it can be argued that some types of forces already have some experience, or they can easily be transformed to swarm-type of forces if the right conditions are in place. As an example, is the Norwegian littoral concept utilizing fast patrol boats (FPBs). These FPBs, operating in numbers from 3-12 vessels, have extensively utilized tactics where they converge on high value targets trying to maximize their total weapon load. Focus has also been on achieving a pulsing effect where the different weapons available on these vessels, missiles, torpedoes and guns have been timely coordinated following relatively simple guidelines from certain weapons release criteria. The existing fleet of FPBs, combined with the newly developed Skjold class FPB, an air cushion catamaran with stealth capacity and a top speed of nearly 60kt, can provide a unique opportunity to develop this force further in a naval doctrine for swarming in the littorals. Unfortunately, the old Hauk class FPBs are to be phased out no later than the year 2010, leaving the remaining FPB fleet with only six new vessels. In light of O'Hanlon's recommendation of retaining older but perfectly usable platforms for further service in the information age, this is regrettable. The Hauk class is newly upgraded and in a swarming type concept a minimum number of units is still required. Consequently, the drive for new technologies and modern sensor weapons can also be a hinder to exploit other doctrinal and organizational sides of the RMA that could give an even better comparative advantage.

Another, and perhaps missed opportunity for developing swarm-type forces, is the newly developed coastal ranger concept. The coastal ranger force, consisting of lightly equipped marine type troops on small high-speed landing craft, is decidedly reduced and integrated in a joint ISTARbn with the army. The unit will function as the ISTARbn maritime element and contribute to security and reconnaissance in the littorals.[131] The costal rangers' limited, but still unique offensive capabilities that rely on speed, stealth, local information knowledge and autonomy in the littorals are apparently to be discontinued. In addition, both the above mentioned forces operate naturally together in the same environment making the degradation of this littoral capability complete when we see them in a combined context.

Similar analogies can perhaps be made for capabilities in the Norwegian army, home guard and air force, but one consequence of this development seems clear; if consistent efforts are not made to adjust the current transformation policies into proper doctrines within a NCW concept Norway will, in few years have a sophisticated but extremely small force structure with severe constraints for doctrinal and organizational development. So far the transformation has been focused on reducing numbers after a "cheese cutter" approach on a broad scale, without properly recognizing that certain capabilities have a critical size limit before their efficiency or endurance drops drastically. In this respect, Alberts reminds us that transformation must be mission specific and concept-driven rather than trailing technology. New information related capabilities must be treated holistically, meaning that they have to be considered in a mission capability context.[132] Breaking up Norway's littoral capabilities in this maritime nation with one of the longest and roughest coastlines in the world, is not a good sign of a holistic approach. In addition, swarming effect operations are not easily conducted within an allied framework due to the particular characteristic of swarming that requires intimate knowledge and long relationships as obtained by training and exercises, before personel are able to operate together. Thus it is important to maintain certain national and comprehensive capabilities.

---

131 Norwegian Chief of Defence, "Forsvarssjefens Militærfaglige Utredning 2003", 18

132 Alberts, *Information Age Transformation*, 36.

With swarm forces and networks in general come also vulnerabilities. Some of these vulnerabilities can be found by studying terrorist organizations such as al-Qaeda that apparently share some of the characteristics of a swarm force. One of the key ideas in this respect is that "it takes networks to fight networks"[133] and we can learn much about future warfighting concepts by studying our enemies who, for many reasons, have fewer constraints applying new technologies and organizational forms to their strategies of war or violence. The relationship between swarming characteristics and some principles on how these networks might be disrupted are depicted in the figure below.[134]

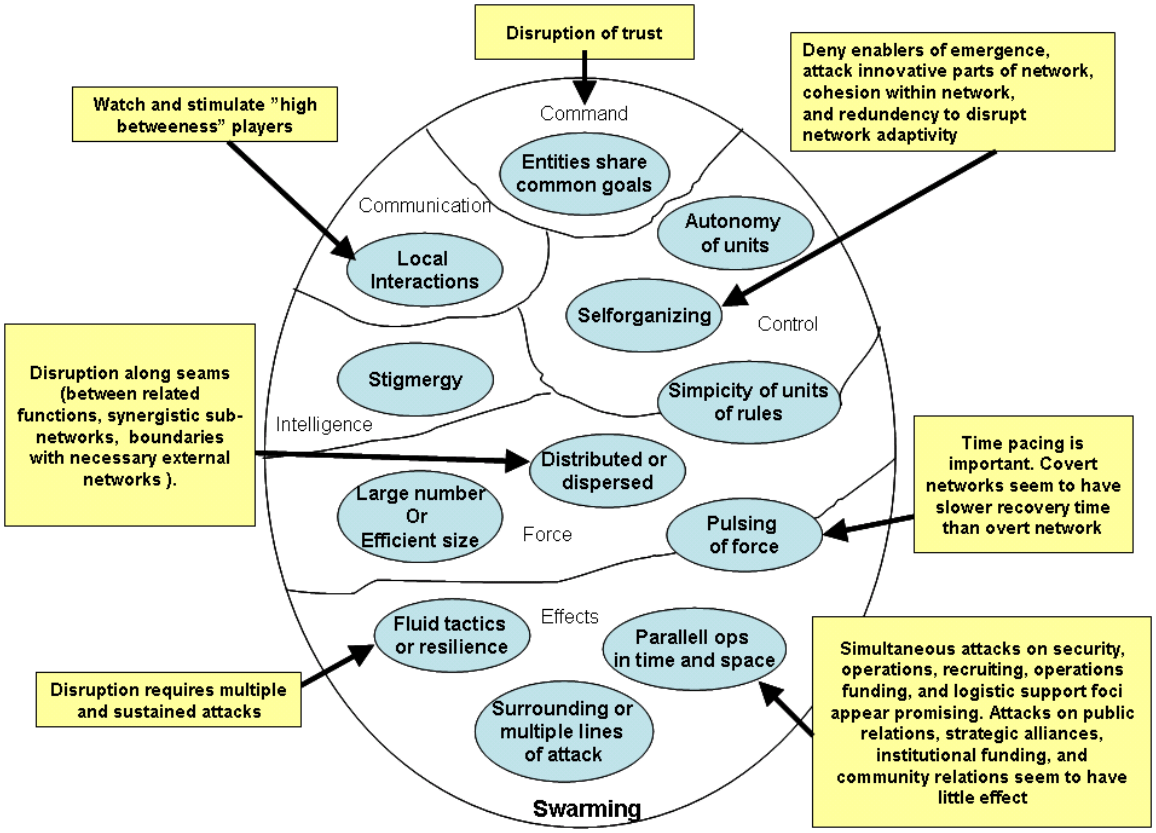

Figure 9. Characteristics of Swarming and Network Countermeasures (From Chartier, Joint C4ISR)

The different concepts of swarming and the implications will not be elaborated further here, although Rheingold's concept of smart mobs in a low-intensity conflict

133 Arquilla and Ronfeldt, *Networks and Netwars*, 15

134 Chris Chartier, "Swarming, Network-Enabled C4ISR, and U.S Military Transformation" in Joint C4ISR Decision Support Center: Conference Proceedings

context will be expanded upon in the next chapter. The reason is that the combination of these two trends in contemporary conflicts has important sociological consequences that deserve to be examined further in a NCW context.

The upper "command area" of Figure 9 also calls attention to the often underestimated function of *trust* in modern societies in general, and in the military command and control systems in particular. In the information age, trust has become so integrated into our daily activities, such as transportation, electronic monetary transactions, e-commerce and so forth, thought is rarely given to the fact that we would not use these systems if we did not inherently trust them. The same can be said for command and control systems. Even more important is the function of trust in information dependent and networked types of organizations. These trust relationships can be interpersonal, sociological, organizational, technological or even system/nation related.[135] A network or organization's use of information to increase its efficiency or achieve its goals is highly affected by whether the information coming through this variety of relationships is trusted or not. Consequently, net-centric forces depending on information superiority should be consciously aware of the function of trust because it will play a significant part if the NCW concept is to function properly. It may be compared to cement in brick constructions. Without trust, NCW would fall apart as a modern way of waging war. Distrust could be compensated for by relying on hierarchical forms of organizations with slow and bureaucratic control mechanisms, or even worse, the technology would not be used effectively nor could information distributed through networks be relied upon. In short, NCW will not work unless people networked and collaborated with, the technology that supports the networks, and the information distributed through the networks are trusted.[136]

Advancing research on the significance of trust in societies and organizations has led to the notion by McEvily, Vincenzo Perrone and Akbar Zaheer to develop trust as an organizing principle. The function of an organizing principle is to solve problems of interdependence and uncertainty and, "is the logic by which work is coordinated and

---

[135] Piotr Sztompka, *Trust: A Sociological Theory* (Cambridge: Cambridge University Press, 1999), 41-45.

[136] Dorothy Denning, dialog with the author at Naval Postgraduate School, 29 April 2004.

information is gathered, disseminated, and processed within and between organizations."[137] McEvily, et.al, see trust as an organizing principle accomplished by "specifying *structuring* and *mobilizing* as two sets of causal pathways through which trust influences several important properties of organizations" (italics added).[138] Furthermore, structuring is explained as:

> …the development, maintenance, and modification of a system of relative positions and links among actors situated in a social space. The result is a network of stable and ongoing interaction patterns, both formal (e.g. routines and organizational units) and informal (e.g. cliques and coalitions). Structuring also creates social stratification that produces differential status, power and knowledge. We argue that trust as an organizing principle molds the social structure of an organizational system in both of these ways.[139]

The other pathway, mobilizing, is explained as follows:

> By mobilizing we mean the process of converting resources into finalized activities performed by interdependent actors. Resources, both material and nonmaterial (such as time, effort attention, and knowledge) are decentralized and unevenly distributed among actors. Mobilizing involves motivating actors to contribute their resources, to combine, coordinate, and use them in joint activities, and to direct them toward the achievement of organizational goals. Mobilizing results in organizational action and, we argue, trust influences the pathway through which such actions arise. Specifically, trust influences the process of knowledge sharing, committing, and safeguarding through the mechanism of disclosing and screening, identifying, and suspending judgment, respectively" [140]

An abstract notion such as trust as an organizing principle may seem like an odd idea, but without trust uncertainty will prevail in information dependent organizations and networks. Also, it is recognized that integration can be achieved by other cognitive-cultural mechanisms. According to Milward and Raab,[141] "These are generally shared

---

[137] Zander and Kogut in Bill McEvily, Vincenzo Perrone and Akbar Zaheer, "Trust as an Organizing Principle", *Organization Science*, Vol.14, No 1, January-February 2003, 91-103.

[138] McEvily, Vincenzo Perrone and Akbar Zaheer, "Trust as an Organizing Principle", *Organization Science*, Vol.14, No 1, January-February 2003, 91.

[139] McEvily et.al, 94

[140] McEvily et.al, 94

[141] H. Brinton Milward and Jörg Raab, "Dark Networks: The structure, Operation, and Performance of International Drug, Terror, and Arms Trafficking Networks" (Paper presented at the International Conference on the Empirical Study of Governance, Management, and Performance Barcelona, Spain, 4-5 October 2002), 21

beliefs within a society outside the organization (common values, common culture, common socialization) and shared beliefs within the organization (common visions, shared norms of cooperation, unity of purpose, corporate identity)." Moreover, and perhaps more important for integration in an allied context is that "a second mechanism which is more intentional and easier to create is the orientation towards common goals."[142] In view of the Iraqi intervention, this last mechanism highlights that reaching these common goals is perhaps not so easy after all. At least it underlines that diplomatic efforts and some level of consensus has to present before operations are conducted in a coalition context.

The key point here is not to introduce an entirely new organizational theory for militaries in the information age, but rather to emphasize that the trust principle at least in coordination with other organizational principles, has the potential to simplify the decision-making process and reduce the need for control. Time and valuable resources may be saved and trust could be part of the answer to reach a state of self-synchronizing forces since, "Trust operates like a 'rule of thumb,' using the information that is available to formulate an expectation, rather than acquiring all of the relevant information to make a comprehensive, rational decision."[143] This quality of trust can be decisive when large amounts of information must be processed in time-sensitive operations. A prerequisite is of course that the actors and technological systems in the different varieties of trust mentioned by Sztompka are trustworthy. That includes allies, other military forces and entities, individual commanders, sensors, weapons and information systems. Blind trust is damaging and will only allow adversaries' countermeasures to work; for instance, attempts of IO, including PSYOPS and deception. Common values, doctrines, language, cultural understanding, interoperable equipment, education and training are some of the key requirements to establish a proper foundation of trust within military organizations and between allies.

Perhaps trust as an organizing principle can support new ways of command and control in the information age. In his closing arguments in the book *Information Age Transformation,* Alberts sees the command and control aspect as a major organizational

142 H. Brinton Milward and Jörg Raab, 21

143 McEvily et.al, 99

challenge and calls for new ideas and research for NCW command and control arrangements. Clearly, they must be different from those developed during the industrial age.[144] The latter were based on staff processes and the supportive technology for command and control. The answer, he argues, may be found by answering three questions. [145] Based on the discussion above, part of the answers may be found in trust:

- Alberts' Q1: Under what circumstances does self-synchronization work?

  Trust contribution: An efficient organization clearly thrives under good trust conditions. A network design must work autonomous within jointly set schedules.[146] Managerial philosophies such as empowerment and structural trust functions will enhance the circumstances where self-synchronisation will work.

- Alberts' Q2: How can command intent be best articulated?

  Trust contribution: Through investments in human capabilities. The more competence in the commander's own organization, "the more facile and effective the network linkages can be made."[147]

- Alberts' Q3: What sorts of command interventions are needed to maintain control?

  Trust contribution: Trust building and maintenance will function as control mechanisms in networks. [148]

Furthermore, Alberts suggests a reconsideration of the whole term "command and control" because it is out of date. Command implies that someone is in charge. Experiences have shown that consultation is the prevalent method and no single entity is actually in charge. Likewise, nobody is responsible for carrying out the intent. A series of collaborative efforts makes the progress. Lastly, control is not an accurate term for describing the level of expected control in today's complex environments and operations. Consequently, Alberts argues that "convergence" is a more realistic goal. These views might seem radical, but they are in line with what Arquilla and Ronfeldt have described as doctrinal practices for netwar actors. Furthermore, these practices align with the early

144 Alberts, *Information Age Transformation*, 140-143

145 Alberts, *Information Age Transformation*, 141

146 Douglas Creed and Raymond Miles, "Trust in Organizations: A conceptual Framework Linking Organizational Forms, Managerial Philosophies, and the Opportunity Costs of Controls" in Roderick Kramer and Tom Tyler (ed), *Trust in Organizations: Frontiers of Theory and Research* (Thousand Oaks: SAGE publications, 1996), 30.

147 Creed and Miles, 31,

148 Creed and Miles, 31

Kosovo experience and the increasingly stronger hands-on approach as a work-around for organizational problems from the U.S. in the later Iraq-Afghanistan coalitions. Thus, Alberts is probably right when he argues that the time is ripe for a re-evaluation of the whole command and control concept if it is to be useful in the information age.

Lastly, actually implementing these organizational paradigm shifts will be an enormous challenge to the traditional Western military hierarchies. Bureaucratic and cultural resistance is an important obstacle to reaching the required goals of new organizational structures. These factors have a more or less universal application in most Western countries. Admiral Owens remarked that "…the promise of the information revolution has stalled as a result of the distraction of world events, poor planning, insufficient budget priority, and behind-the-scenes bureaucratic opposition to the dramatic organizational and cultural changes…"[149] For the British there is a preference for close combat warfighting concepts and an innate reluctance to embrace the RMA based on the nation's and the military's culture.[150] Similar resistance is experienced in Norway, and the Minister of Defense is particularly stressing this point since the whole defense structure, including the military must embody both the will and the ability to change and adapt in order to achieve the aims of the transformation process.[151] Consequently, this will and ability must be founded in a clear and understood vision of the NCW concept if transformation is to succeed.

C. MISSION CHALLENGES IN CONTEMPORARY CONFLICTS

The lessons learned in the contemporary conflicts in Afghanistan and Iraq are predestined to influence the development of Western militaries. Thus, some experiences from these contemporary conflicts thought to be particularly relevant in the discussion of mission challenges based on changes in the nature of conflict have been highlighted in this section.

---

[149] Bill Owens, *Lifting the Fog of War.* (New York: Farrar, Straus and Giroux, 2002), 208

[150] David Potts and Jake Thackray, *The Big Issue: Command and Combat in The Information Age* 2 and 29-30

[151] Norwegian MoD, "The Further Modernization of the Norwegian Armed Forces 2005-2008", Proposition to Parliament No. 42 (2003-2004) Short Version, *5*

1. NCW as a Problem Fixer

An important challenge in the transition to information age militaries is the exaggerated belief in new warfighting concepts and technologies as problem fixers without taking into consideration that the basics in the nature of war, in fact, are unchanging. Although Alberts et.al., reject the notion that NCW will change the nature of war profoundly,[152] for many scholars it is a concern that a non-linear approach to warfare utilizing superior information technology and a system of systems approach to lift the "fog of war" in accordance to, for instance Admiral Owens visions,[153] will lead to the perception that classical strategic thought is outdated. Concerns are raised that exaggerated belief in NCW will reduce the art of war to science, that the operational art will diminish with increased centralization of command and control until NCW is nothing more than a tactical concept, that the enemy's countermeasures will not really matter and that the role of morale and psychological factors will no longer have an impact.[154] The latter arguments, somewhat simplified, were stated by Dr. Vego in his article "Net-Centric Is Not Decisive."

Vego's concerns might be right in view of how Western militaries actually are performing in contemporary conflicts. In the Iraqi case, criticism has been raised because the administration and campaign planners neglected to plan the post-combat phase properly. "The U.S. was woefully unprepared for the postwar administration of the country and was surprised by the extent of the guerilla war that it would have to fight."[155] In light of NCW characteristics, one can argue that planners applied a nonlinear approach with a tactical focus on the whole Iraqi problem. Hence, proper phasing was deemed unnecessary and the campaign was seen as a continuous operation, which arguably promotes higher tempo and more flexibility in the conduct of operations. Although it is difficult to tell with certainty, at least with the advantage of hindsight, many of the encountered problems now facing the U.S. led coalition could have been approached

---

[152] Alberts et.al, *Network Centric Warfare*, 7

[153] Owens, *Lifting the Fog of War*. 202.

[154] Milan Vego, "Net-Centric Is Not Decisive", *Proceedings*, January 2003

[155] Shawcross, 233.

differently on the basis of a more thorough planning preparation for the post-combat phase.

2. Shortcutting Strategies

Another important lesson comes from the alleged exaggerated belief by the current U.S. administration and the media that as soon Saddam Hussein's regime was toppled, and the dictator himself captured, the necessary grounds for the Iraqis to stop the resistance, begin nation-building, and embrace democracy would be created. Surprisingly to many it was not, or as expressed by the Secretary General of the UN., Kofi Annan "People are happy Saddam has gone, but they had not expected this disorder to follow".[156] This simplified cause and effect relationship of decapitation strategies, coupled with a convincing, but also true, belief in the information enabled U.S. supremacy on the conventional battlefield, highlights the danger of shortcutting strategies that promise fast solutions to difficult problems. In the Iraqi case it might also have suppressed the U.S. administration's view of the need for diplomatic efforts for the purpose of having a larger portion of the international community onboard. Clearly this was a campaign U.S. forces could undertake alone if they had to. The consequences of not fighting harder along the lines of diplomacy seem clearer today when several countries have announced that they are pulling out from Iraq in the summer of 2004. The tactical consequences of these withdrawals are perhaps insignificant, but within an allied network they should be regarded as very serious. As a global actor, the U.S. needs these allies regardless of how small their contributions are, and conversely, smaller nations still need a strong, trustworthy and competent ally like the U.S. with sustained confidence in the world community. Indeed, the post-combat phase in Iraq, where democratization is the main objective, will be a test for modern democracies, gauging how future conflicts will evolve. Clearly the objective of spreading democracy should be an international venture.

[156] Cited in Shawcross, 220.

3. Identifying Tipping Points

A third lesson from Iraq is the highlighting of the moment of Saddam's capture as the tipping point in the liberation of Iraq. Although several media recognized the significance of this event, particularly one article by Frank J. Gaffney Jr. in the *Washington Times* specifically used the term "tipping point" to describe the situation.[157] Four months after the capture, when this was written, severe fighting broke loose in the Sunni Muslim dominated city of Falluja, and there is substantial fear that the unrest will spread to other regions as well. In addition, insurgent bomb attacks and kidnappings of foreign military and civilian personnel are presently increasing. Creating a tipping point in a conflict or any other desired/undesired social behavior is of course wanted, but they rarely occur by wishful thinking, or simplified cause and effect analyses that particularly are found in decapitation strategies. True tipping points are hard to predict because the cause and effect relations in social behavior are immensely complex. The concept of tipping points originates in epidemiology and can be described as the idea "that small changes will have little or no effect until a critical mass is reached."[158] Figuratively, and with implication for social behavior, the term implies that when certain social or structural conditions are in place, just a small incident is enough for the situation to tip in a particular direction. A tipping point has three characteristics: "…one, contagiousness; two, the fact that little causes can have big effects; and three, that change happens not gradually but at one dramatic moment…"[159]

Saddam's capture was obviously an important victory for the coalition forces, but at that phase of the occupation, Saddam's power of influence was definitively over. One could argue that it could be equally dangerous to underestimate the myth and inspiration of Saddam's legacy, but the possibilities that the insurgents' cause rests more on other factors such as Islamic fundamentalism and anti-Americanism rather than support to Saddam himself should perhaps have been emphasized more. Added to the equation is also the influence and activities of other adversaries, for instance al-Qaeda, which were not traditionally affiliated with the Baath regime. Moreover, the event was not likely to

[157] Frank J. Gaffney Jr. "The Tipping Point". *Washington Times*, 16 Dec 2003. http://nl.newsbank.com/nl-search/we/Archives?p_action=list&p_topdoc=11 (accessed 22 April 2004).

[158] Neil Swidey, "Tipping Points: How Military Occupations Sour", *Boston Globe*, April 27, 2003.

[159] Malcolm Gladwell, *The Tipping Point* (Boston: Little, Brown and Company, 2000, 2002), 9

change the average Iraqi citizen's everyday life. More essential was the occupation forces' attitude and efforts to improve overall security, critical infrastructure and living conditions in general. In other words, to deliberately create a tipping point the occupation force should focus on networks in the population that will make the difference with regard to the critical mass. Hence, resources must be freed to attend the symptoms of dissatisfaction by improving the small and everyday changes rather than focus on the big issues. Simultaneously, obvious hostile groups in the population must be contained or eliminated. To create a contagious effect the local politicians, religious leaders, connectors, mavens, salesmen, and other gatekeepers must be influenced. In this respect the word of mouth is more important than advanced information technology, international headlines and governmental statements. Hence, any surpluses in information advantage or military resources should be used to create conditions for changes at the level of ordinary citizens, or in the influencing part of the population, in order to reach the critical mass in which a tipping point can occur.

4. Integrated Civilian and Military strategies - Tipping Points Continued

In military terms a tipping point resembles, but is not equal to, the culminating point that planners and commanders try to identify, avoid or establish the conditions for in different phase of a campaign. Certain criteria are identified to indicate when own or the enemy's culmination point can be expected to occur. The culmination point is traditionally connected to the offense where the goal is to maintain the initiative and momentum in an operation. In light of the characteristics of low intensity conflicts and expected information superiority, perhaps the culmination point should be redefined to also include the characteristics of a tipping point. Due to its complexity it would be harder to identify and many aspects of the necessary conditions needed to reach such a point would be out of military control. Traditionally, external interference is regarded as disadvantageous by the militaries but such an approach will at least highlight the need for better interagency and NGO cooperation or even full integration. The British counterinsurgency strategy in Malaya serves as a classical example for successful military-civilian integration. This strategy was not primarily military, but as R. W. Komer

points out, "a mixed strategy encompassing civil, police, military, and psychological warfare programs, all within the context of a firm rule of law and steady progress toward self-government and independence, which robbed the insurgency of much political appeal."[160] A mixed or integrated strategy does not imply limitations on offensive and proactive means where commanders deem it necessary, but it would highlight the defense, phasing, planned operational pauses and preventive strategies to a larger degree.

Moreover, the dangers of a nonlinear approach where the decision makers lose sight of the larger problems and objectives may be reduced, or as Vego puts it, "Campaigns and major operations normally are divided into several phases because the ultimate objective cannot be accomplished in a single fell swoop, even against a much weaker opponent. Without phasing, there is the risk of overshooting the point of culmination"[161] Thus, understanding and identifying tipping points is a very good incentive to develop truly integrated civilian-military strategies in future conflicts, and particularly in low-intensity conflicts. Such analyses can be a very powerful tool in a NCW concept where all the resources, military as well as civilian, to a larger or lesser degree must be integrated to reach common goals.

5. Evolving or Revolutionary Nontraditional Missions?

Another important mission challenge is the neglected military view on low intensity conflicts as "worthy" military missions. Obviously there is reluctance in the military to embrace these new and changing missions such as peace support and humanitarian operations even if they have political, economic and social significance. The current conflicts in Afghanistan and Iraq are both in a low-intensity phase with an apparent asymmetry between conventional coalition forces and local insurgencies or terrorists. As recently discussed, there are problems applying military power effectively against these adversaries. The expected dividends of information superiority have been markedly absent against these types of adversaries. The exception is perhaps found in the "Afghan model," at least in the first phases of the Afghanistan war where an

[160] Robert W. Komer, *The Malayan Emergency in Retrospect: Organization of A Successful Counterinsurgency Effort* (Santa Monica: Rand R-957-ARPA, February 1972), v.

[161] Vego

unconventional approach utilizing coalition Special Forces, combined with precision munitions and an indigenous ally, proved to be highly efficient against the Taliban regime and al-Qaeda fighters.[162] Later, when conventional forces dominated the Afghan battle space, and when the enemy had turned unconventional, progress was halted. This does not imply that Special Forces and/or the Afghan model are the only possible solution to low-intensity conflicts or insurgency problems, but it does suggest that different types of conflicts need different solutions and sets of forces. It also suggests that counter guerrilla warfare in particular needs unconventional approaches to succeed. Although low intensity conflicts and new asymmetric threats are addressed in, for instance, NATO's strategic concept,[163] and in many Western countries' military doctrines, the preferred solution still seems to be a conventional approach. In the Afghan case, one could argue that the initial extensive use of Special Forces was a choice of necessity more than a preferred course of action. At the time, nobody else was capable of doing the job within the critical time limits and logistical challenges that the Afghan battle space represented. The key to success, however, "is to team heavy, well-directed fires with skilled ground maneuver to exploit their effects and overwhelm the surviving enemy,"[164] in addition to a sound strategy to recruit skilled and local allies and gain popular support. The latter is perhaps a greater challenge than the former in future low-intensity conflicts.

The reluctance to adapt militaries based on changes in the nature of war is nothing new. In 1991, due to new threats and the emergence of low-intensity conflicts with vastly different actors such as terrorists, guerillas, bandits, robbers and other non state actors, Van Creveld stated the need to reevaluate the nature of war in our time.[165] To the extreme he argued that "If, as seems to be the case, the state cannot defend itself effectively against internal or external low-intensity conflict, then clearly it does not have a future in front of it."[166] Liddell Hart made the same observations almost 30 years

---

[162] Stephen Biddle, "Afghanistan and the Future of Warfare: Implications for Army and Defence Policy", (U.S. Army War College, Strategic Studies Institute, November 2002), vii.

[163] NATO, "The Alliance's Strategic Concept".

[164] Biddle, viii.

[165] Martin Van Creveld, *The Transformation of War* (New York: The Free Press, 1991), 222.

[166] Van Creveld, 98.

earlier in his second revised edition of "*Strategy*" where he included a chapter on guerilla warfare in which he added a clause to his old maxim; "If you wish for peace, understand war - *particularly the guerilla and subversive forms of war*"[167] (italics added). Furthermore, he argued that conventional responses to these conflicts, utilizing overwhelming forces and strategic bombing are counterproductive and in fact enhance guerilla type strategies.[168] Like Van Creveld, he saw the need for a reorientation of military policy to develop counter strategies of corresponding kind to face this new threat.

Noticeably, there is a need to transform both the understanding of low-intensity conflicts as Van Creveld claims and war fighting capabilities to meet the information revolution, as RMA proponents suggest. Applying RMA only to the conventional, mid- and high intensity level of war will not help solve the difficult problems connected to low-intensity conflicts. Moreover, the scale of conflict is not a continuous line with just a higher intensity of the same problem. High-and low-intensity conflicts are in fact inverse problems with vastly different origins and threat assessments. They require different strategies, tactics and organizations in order to be solved.[169] Recognizing this diversity should imply that both capabilities are needed and that the types of forces employed in each case are not necessarily easily compatible, at least not without an extensive period of combat enhancement training prior to insertion.

Likewise, it would be a waste not to exploit the anticipated information superiority based on new information technology to also enhance the counterterrorism or counterinsurgency strategy and tactics. For sure, when found convenient and secure enough, adversaries such as insurgents and terrorists will utilize all means in their power to achieve their objectives. As will be discussed later, cyberspace is not an unfamiliar sphere for extremists, terrorists and insurgents. The potential impact of the latest trends in the information revolution on adversaries in low-intensity conflicts should be equally, if not more, emphasized when developing and implementing a NCW concept. The impact of the information age will be in force in all types of low-intensity conflicts but most

---

[167] Basil H. Liddell Hart, *Strategy,* (London: Meridian, 1991), 361.

[168] Liddell Hart, 364.

[169] Gordon McCormick, Naval Postgraduate School: Lecture in Guerilla Warfare, 7 September, 2003.

urgent is the al-Qaeda type terrorist threat and insurgencies as they are seen in Afghanistan and Iraq. Currently, they represent the most serious threat against Western values and democracy, and at least some types of terrorist organizations clearly know how to operate in a high tech environment.

This reemphasizes the dangers in exaggerating our faith in new warfighting concepts and also Liddell Hart's warning that certain (conventional) preferred strategies and tactics can be counterproductive against terrorists and insurgents. Militaries in the information age should ensure that the newly developed forms of warfare, such as rapid decisive operations, knowledge-based warfare, information warfare and shock warfare aiming to strengthen the offense, do not become equally counterproductive. As will be discussed later, there are several areas in which an adversary may exploit new information technologies. Consequently, the defense should be as equally emphasized as the offense in order to ensure that proper capabilities exist to maintain equilibrium between the two.

D. THE IMPACT OF INFORMATION SUPERIORITY

Several mission challenges and constraints arise with the concept of information superiority. As dangerous as exaggerated beliefs in superior strategies and military strength is an overestimation of the effects of information superiority. For instance, in the Kosovo war, NATO's information supremacy did not achieve a political or diplomatic victory. Neither did it give NATO major operational or tactical advantages. Instead, the assumed knowledge led to an overestimation of NATO's capabilities, and information also become subject to Serbian manipulation.[170] Consequently, despite of information-sharing progress within the coalition forces, the Kosovo experience showed that NATO had a long way ahead before it could fully exploit advances in information technology, and the campaign highlighted the urgency for improvements.[171] The approach is,

[170] Timothy L. Thomas, "Kosovo and the Current Myth of Information Superiority", *Parameters*, Spring 2000.

[171] Larry Wentz, *Lessons from Kosovo* (CCRP publication series, July 2002), 672.

however, "a matter of political will rather than a technology solution. Technology will only be an enabler." [172]

Also, the concept of IS, as explained in Chapter Two, involves the gathering, processing and distribution of enormous amounts of data. In addition, networking the forces is expected to increase the value of information significantly. Metcalf's law states that "as the number of nodes in a network increases linearly, the potential 'value or effectiveness' of the network increases exponentially as the square number of nodes in the network."[173] However, there are pitfalls connected to the increased information richness that ought to be considered in a NCW implementation.

The following will elaborate a few of the constraints and pitfalls of information superiority since they undoubtedly will have an impact on the NCW concept.

1. Impact on the Decision Making Process

Thus, what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is FOREKNOWLEDGE.

Sun Tzu

In general, processed military information should be presented in a Common Operational Picture (COP) enabling different friendly actors shared and increased situation awareness. In turn this common awareness enhances collaboration and synchronization within the force. Moreover, the amounts of information that are possible to integrate in the COP are almost infinite, but along with the information richness emerge several problems.

The first lies in the danger of information overload. Until machines are able to reasonably simulate complex systems in a digital and virtual conflict environment, it still takes a human brain to analyze the essence of the information and transform the information into relevant decisions on the battlefield. Although future technology enables more and more information processes, as well as decision-making processes to be automated, machines still have limited functions in the cognitive domain. This is

[172] Wentz, 672

[173] Alberts, et al., *Network Centric Warfare,* 32.

especially true for decision-making processes that are connected to the adversary's intent and future courses of action. Often, factors like psychology, intuition and educated guesses are more important to a commander trying to figure out several sequential moves in an adversary's unpredictable strategy. In these cases it may be more productive to simplify and reduce information to get to the core of the problem.

Secondly, when all levels have access to the same planning assumptions and real time information/intelligence, it can result in a common problem focus and blur the distinction between the tactical, operational and strategic levels. Although technical solutions provide the capability to filter and adjust the COP to each commander's needs at various levels, it is within human nature to gather and present as much information as possible. This tendency may actually be counterproductive compared to the desired speed and self-synchronization in NCW. Hence, organizational as well as technological mechanisms must be found to prevent commanders relying on the same COP that cannot be shared nor real at all three operational levels simultaneously, according to the intended functions of these levels.

The third problem lies with the anticipated advantage of speed in the decision making process. Ultimately IS means to improve our own OODA loop[174] compared to an adversary's. Arguably, the dividend of IS is highly focused on responding more quickly, for instance by shooting faster and more accurately at the enemy. However, it can be argued that the improvements should be more focused on the *observe* and *orient* portion of the loop. Self-synchronization and speed in the decision making process may lead to hastened and unintentional responses. The technical advanced AEGIS cruiser, USS Vincennes, shoot-down of Iran Air Flight 655, 3 July 1988, killing 290 people, may serve as an example of the consequences when critical decision making processes, based on advanced information technology are short-circuited in the drive for speed. The shoot-down happened after the airliner had crossed the 20-mile point where the commander of USS Vincennes had announced that he would shoot if it did not change course.[175] Apparently, the pilot of Flight 655 never received the warnings. Although this case

[174] OODA loop: Observe - Orient – Decide - Act

[175] David Evans, "Vincennes ", http://www.odu.edu/webroot/orgs/ao/mo/nrotc.nsf/files/Vincennes.PDF/$FILE/Vincennes.PDF , (Not dated) (accessed 24 April 2004).

involves many aspects, including an alleged offensive mentality of Vincennes' commander, the shoot-down clearly highlights the complexity of time sensitive decision making, including automated decision making processes and the human mind's role in modern C2. The incident also highlights self-synchronization issues including delegation of authority and proper rules of engagements. Lastly, the Vincennes' case highlights force protection issues and the appropriateness of using the right set of forces and technology for a particular mission. The question is if the cruiser, a highly specialized air defense platform, was the right choice to operate within Iranian littorals in the first place, considering the threat that consisted of low-tech Iranian gun boats with very limited weapon capabilities.

Fourth, IS may imply that we outthought ourselves in the decision making process. Adversaries that do not rely heavily on IT, have been denied information or have been denied access to his own information systems, may not even have perceived our first moves when we start a second OODA loop. When we initiate our second move he might respond on our previous moves leaving us with the wrong impressions of cause and effects. Hence, asymmetry of perception can be counterproductive to our objectives, particularly in Military Operations Other Than War (MOOTW). Understanding the limitations of Information Superiority is therefore just as important as understanding its possibilities. IS will never be a 100% condition because then we must understand our adversary's cognitive domain to the full, which is practically unachievable.

Similarly, the expediency of a strategy that aims to degrade an opponent's information and information system indiscriminately is questionable, and even if efforts are made to discriminate, the impact of information is difficult to control and measure since it ultimately is processed in the cognitive domain. Denying a foe information will consequently allow other perceptions, also false ones, the freedom to operate. Information gaps will be replaced by more or less qualified assumptions. Thus, IS, within the concepts of IO, should incorporate plans for information sharing; not only to friends and allies, but to opponents as well. Again, this is particularly important in MOOTW where "the military should use its mighty information technology to generate the "00" portion of the decision-making loop for others who ultimately will take the lead in

deciding and acting."[176] In addition, civilian and military information structures are tightly shared structures,[177]which also brings about the problems of collateral damage and the usefulness of the very same structures for our own purposes, for instance in nation building efforts.

Conclusively, one lesson for developing information age decision making processes is that, "…the point is not to engage in some never-ending speed race with our own worts-case fears, but rather to concentrate NCW on how to best exploit the delta between our loop time and his."[178]

2. Information Superiority and Asymmetric Responses

Attack him where he is unprepared, appear where you are not expected.

Sun Tzu

It is also a concern that IS and improved technology will encourage asymmetric responses. It will not only be U.S. allies that will find it problematic to follow such a costly path. Third world countries, rogue states, sub state organizations and terrorists will obviously lack the resources to match U.S. forces on the battlefield with equally symmetric responses. Instead, they will seek to use asymmetric responses, such as guerrilla warfare, cyberattack, information warfare, terrorism tactics, and WMD if their position is threatened. Nothing is more dangerous than a cornered opponent. Feeling total inferiority and denied influence through, for instance, IO, may force an opponent to his limit where tactics and weapons such as terrorism and WMD seem the only solution to deter U.S. or coalition forces from further intervention.

Asymmetric responses also move the costs of warfare away from advanced technology and military forces to other dimensions.[179] In guerrilla warfare, the costs are transferred to human and social dimensions. The civil population will come in harm's way and infrastructure will be destroyed. In addition, because these types of operations

[176] Barnett, "The Seven Deadly Sins of Network-Centric Warfare".

[177] Dorothy E Denning, *Information Warfare and Security,* (ACM Press Books, 1999), 17.

[178] Barnett, "The Seven Deadly Sins of Network-Centric Warfare"

[179] Ragnar Solstrand, "Teknologi, Forsvar og Forsvarsstrukturer", (Norwegian Defense Institute, 2000 - Report 2000/03429), 24.

often are risky and long-lasting, it may be difficult within a coalition to recruit and sustain operations. Other types of asymmetric warfare may have other cost attributes depending on the nation or actor involved.

In addition, if one's force consists of few and costly units it might create a higher threshold to use them. Consequently, a commander will closely consider the risk of using high value units before they are put into action. Added to the equation is also the emerging trend in the U.S. and other Western countries that a military's own casualties must be kept at a minimum to sustain political and public support to a military campaign. In particular, this would be applicable in low-intensity conflicts. Recent conflicts such as the first Gulf War, Kosovo and Somalia have proven this as a considerable factor that limited the coalition's efficiency and end-state objectives. It should be noted that in other cases, the Western and particularly U.S. risk-adverse mentality have been overestimated by adversaries. The willingness to take risks is, ultimately, closely linked to how vital the interests are perceived. This lesson will surely be remembered by Osama bin Laden and Saddam Hussein. The key point is, however, that IS has little value if the information cannot be properly exploited, for instance, as in Kosovo, by not flying low enough or putting troops on the ground to counter an identified target.

Lastly, assuming knowledge as IS implies might be dangerous when countering an asymmetric opponent. It is not a given that IS will increase because the opponent is less dependent on IT. Asymmetric responses will always seek to exploit vulnerabilities. Less IT might just as well imply "greater social capacity for low-tech work-arounds that either negate or complicate information warfare immeasurably."[180] Such work-arounds were frequently experienced and exploited by the Serbs during the Kosovo conflict, which by many was said to be a conflict where NATO had near IS. Wesley Clarke pointed out one such vulnerability on the public-relations front, "…we knew that NATO's greatest vulnerability was unintentional injuries to innocent civilians. We knew the political impact on our governments could be devastating if it were thought that innocent civilians were inadvertently bearing the brunt of NATO's air attacks."[181] Furthermore, the Serbian forces managed to manipulate NATO's battle space awareness

[180] Barnett, "The Seven Deadly Sins of Network-Centric Warfare".

[181] Wesley Clarke, *Waging Modern War* (New York: PublicAffairs, 2001), 296

far more often than expected.[182] Due to human and software failure to interpret intelligence information, bad assessments of the actual situation were made, resulting in wasted ammunition on fake or inaccurate targets. Other work-arounds might exploit another great weaknesses; targeting civilian personnel or objects in the homeland, in coalition territory or even in a third country. Such strategies and tactics will increase the battlespace significantly. In the U.S. it already has with the establishment of the Department of Homeland Defense. This is a true paradigm shift for a country that had never experienced any external threat since its origin.

3. Increased Political Interference in Military Operations

"Thus it may be known that the leader of armies is the arbiter of the people's fate, the man on whom it depends whether the nation shall be in peace or peril."

Sun Tzu

Information Superiority also implies that detailed information is available to all decision makers in the chain of command as well as to the politicians. Political control of the military is a cornerstone value in most Western democracies. However, detailed political control at the operational and tactical level may severely hamper military operations. Therefore, IS, which includes the ability to transfer live audio and video, or by other means visualize the actions on the battlefield, may tempt politicians to introduce an extra decision making loop before resources are assigned to operations. Negative effects of such interference could be that the commander's own decision making loop will increase instead of shorten. Another implication is that interference may disrupt military campaigns and the targeting process, which are logic and often sequential processes with the intent to decrease the adversary's military capabilities systematically. Furthermore, it is always a prerequisite that these campaigns have been through a political process where the intent, objectives and end-states of an operation have been made clear and politically approved. Consequently, and even if a tighter interagency cooperation and integration are deemed more important in the future, detailed political

[182] Thomas, "Kosovo and the Current Myth of Information Superiority".

interference should be unnecessary. If it occurs, it may diminish both the short- and long term effect of military operations.

Also, interference may actually hamper IS and put forces at considerable risk. In Kosovo, the effectiveness of information systems was actually degraded because the politicians demanded that pilots fly above a certain height to minimize casualties.[183] Moreover, inconsistent and changing political objectives reduce the advantages of a commander's campaign planning, which exploits available information systematically and comprehensively. In the Kosovo campaign these objectives changed progressively from the air campaigns' initial aim of bringing Milosevic back to the negotiating table, to stopping the ethnic cleansing, to ceasing fire, to Serbian withdrawal and return of refugees, and finally, to the presence of a NATO led international force in Kosovo.[184] It is therefore important that new and adequate ways to integrate the political process are found when developing the concept of IS. If ways around this problem in limited wars or low-intensity conflicts are not found, IS might actually be counterproductive to the goal.

4. Increased Vulnerability in Cyberspace

"*We repeat then that the defense is the stronger form of war, the one that makes the enemy's defeat more certain."*

Clausewitz

Increased dependency on sophisticated information systems to achieve IS will inevitably entail greater vulnerability to the same systems. Information systems can be influenced in the physical, information, and cognitive domain. The two latter include the use of Cyberspace for influence; and, it is not unreasonable to claim that the battles in these domains increasingly will be fought in Cyberspace. In this respect, the Institute for Security Technology Studies at Dartmouth College points out three lessons learned after studying the India – Pakistan conflict, the Israel – Palestine conflict, the Kosovo conflict,

183 Thomas.

184 Wesley Clarke, *Waging Modern War* (New York: PublicAffairs, 2001), 423-424

and also the tension that occurred between the U.S and China over the U.S. surveillance aircraft incident. The lessons are:[185]

- Cyber attacks immediately accompany physical attacks
- Cyber attacks are increasing in volume, sophistication and coordination
- Cyber attackers are attracted to high value targets

These general trends apply to all kinds of cyber attacks, with or without political motivation. Other hostile actors in cyberspace, with different motives, can be criminals and thrill seekers or "script kiddies".

It is appropriate to anticipate similar types of cyberattack in future conflicts. However, as the lessons learned point out, the attacks may be expected to be more severe, aimed not only to spread a political message, but also to influence, or destroy information systems and other vital IT based infrastructure. Even if military systems may be better protected and easier to isolate military operations will be, directly or indirectly, influenced by cyberattacks on the civilian society. For instance, over 95% of military communications are routed over civilian links,[186] which obviously could hamper military operations if these links were attacked either physically or through cyberspace.

It may be very difficult to control information and gain IS in a cyberwar scenario. Conflicts draw attention from a variety of groups with more or less peripheral interests and connection to the conflict itself. Thus, the participation in a cyberwar against a Western coalition during conflict may be high. Pro-opponent hacker groups and activists may align their efforts and launch coordinated cyber attacks. Likewise, peace, or otherwise motivated activists, may also coordinate similar types of cyberattacks simultaneously. In a worst-case scenario, the attacks will come from several directions causing a swarming effect. This may be intentional or unintentional, but the effect can be dangerous as the magnitude of attacks may hide and take away information managers' focus from more severe cyberattacks.

---

185 Trustees of Dartmouth College, "Cyber Attacks During the War on Terrorism: A predictive Analysis", 1.

186 Denning, Dorothy E. *Information Warfare and Security*. (ACM Press Books, 1999), 17.

Consequently, some of the threats IS should encompass defense against are:[187]

- Frequent and massive cyber attacks with activists and hackers using swarming techniques
- Attempts to deface governmental, military and other institutional web sites. These attacks will be politically motivated aimed to disseminate false information and propaganda
- Distributed Denial of Service (DDoS) attacks. These attacks can be very severe if aimed at vital societal infrastructure
- Worms and virus attacks. New and more devastating worms are being developed. Some may spread in a very short time before countermeasures can be developed. Others may have a sleep phase, which enables them to coordinate an attack. Combined with a physical terrorist attack, these worms can have a devastating effect.
- Exploitation of routing vulnerabilities.
- Infrastructure attacks. Unauthorized intrusion of vital infrastructure resulting in infrastructure outage and corruption of information. Combined with terrorist attacks, this might be the most devastating type of cyber attack.
- Compound attack. A mix of the above points and/or combined with physical terrorist attacks.

Vulnerabilities to other and more direct military threats, such as physical attacks, jamming, use of EMP and/or directed energy weapons, insiders and spies, are also a concern. For instance, it is believed that Milosevic had an insider within NATO during the bombing campaign. The insider notified Belgrade, reducing the effect of bombing, because targets where either moved or replaced by dummy targets[188]. These vulnerabilities are not new and spies have existed just as long as military conflicts have. The problem now is that excessive belief in, and reliance on IS as the enabling factor for strategic and operational concepts, may have more fatal consequences than before.

To summarize, in future conflicts the potential number of hactivists, hackers and other cyber warriors against sophisticated but also vulnerable Western militaries have a mobilization potential never experienced before. In addition, and partly because of the link to the disputed U.S. led strategies against GWOT and WMD, a cyberwar can be

[187] Trustees of Dartmouth College,. "Cyber Attacks During the War on Terrorism: A predictive Analysis", 14 - 18.

[188] Thomas.

expected to be more sophisticated and devastating than previously experienced. Hence, information assurance as part of IO to prevent the above mentioned threats is essential to enhance confidence in proprietary information and to achieve and maintain IS.

E. CONCLUSION

This chapter has focused on changes in the nature of conflict based on characteristic developments in the information age. Some of these changes will have an important impact on the mission challenges, opportunities and constraints in future forms of war. The characteristics of these changes should be carefully considered in an NCW implantation. One important conclusion is the need to emphasize nontraditional missions that occur in low-intensity conflicts, humanitarian crises, terrorist and criminal activities. The perfection of traditional combat never will be good enough in order to sufficiently reduce the costs of war, but it is not in this arena that Western countries are facing the most important challenges in the future.

Furthermore, organizational and doctrinal challenges that are foreseen in new and unique forms of war in the information age should be paid more attention to than blending new technologies. In this regard, holistically net-centric and information capabilities that are mission specific should be developed. Mission capability packages, such as Norway's vital need to maintain a warfighting capability in the littorals, must consist of an appropriate operational concept, including new information age doctrines for command, control and organization. The force structure should be adequately equipped to operate in an information and time sensitive environment; be efficiently organized and sized to have the adaptability to develop and incorporate new concepts such as swarming; and lastly, human capability development should be emphasized through adequate education and training. In addition, networks are highly trust dependent and the development and maintenance of trust is seen as increasingly more important for net-centric forces to operate. Trust functions, in military organizations, should be studied as a contribution to finding more suitable command and control arrangements within NCW concepts.

Other mission challenges, opportunities and constraints also arise as a consequence of changes in the nature of conflict. Arguably, examples from contemporary conflicts show a tendency to view new warfighting concepts as problem fixers and exaggerate conventional and technological supremacy on the battlefield. In doing so there is a danger to overlook causal relationships, especially in low-intensity conflicts. This tendency may shortcut strategies and lead to unintended consequences. Likewise, there are also pitfalls related to the concept of information superiority. This enabling concept will eventually reach its potential when military forces mature in a fully networked and joint environment. That may still take years. Ironically, it will not be the missing gaps in new information technology that will be the greatest hindrance, but rather our own ability to reorganize, cooperate and comprehend the true nature of information as power on the same level as other warfare areas.

Lastly, NCW does not represent a new theory of war by the standards of historical or empirical evidence although the first part of the Afghanistan war was a good test of network-style operations. Hence, an overestimation of the concept can be equally dangerous as not taking it into account. Nevertheless, changes in the nature of conflict, only a few aspects of which were discussed in this chapter, have[189] and should lead to a further redefinition of the principles of war for information age forces. The principles networked actors rely on to achieve precise and decisive results are based on superior knowledge and must be different from the principles currently defined in contemporary doctrines based on attrition- or maneuver-warfare. By emphasizing the conceptual, doctrinal and organizational aspects in a NCW implementation we should be able to develop these principles further.

[189] See, for instance, Robert R. Leonhard's, *The Principles of War for the Information Age* (New York: Ballantine Books, 1998)

THIS PAGE INTENTIONALLY LEFT BLANK

V. LOW INTENSITY CONFLICTS AND EMERGING TRENDS IN THE INFORMATION AGE

Previously, the needs of transformation of both the understanding of low-intensity conflicts and war fighting capabilities to meet the information revolution have been pointed out. The last Chapter Four highlighted some of the factors that may contribute to such an understanding. Still, a more in-depth analysis is needed to understand the impact of the information revolution on potential adversaries. So far, the practical experiences of the RMA has been relatively internal for Western military organizations trying to exploit the advantages posed by new information technology within existing doctrines. Nevertheless, the same technologies and organizational progresses apply to other actors in low-intensity conflicts as well. In addition, the developments in new information technology are continuing in quantitative leaps rather than in a continuous and predictable manner. The strategic and sociological consequences of these developments are hard to predict. Networked type of organizations, wireless technologies and peer-to-peer (P2P) communications have been, and will probably continue to be, employed by extremists, terrorists and insurgents in the future. This chapter will analyze some of the newest trends in the information age coupled with old and new theories on how terrorists and insurgents operate. The result of such an analysis may contribute to developing NCW capabilities that will be more useful than the ones being applied today in these evolving nontraditional missions. A key question is whether actors such as terrorists and guerrillas operating as "smart mobs" will be seen in netwars where the main battles will be fought in the information and cognitive domain rather than in the traditional physical space.

A. LOW INTENSITY CONFLICTS - THE DOMINANT FORM OF WAR

According to Martin Van Creveld, three-fourths of all armed conflicts since 1945 have been low intensity conflicts (LIC) and have also tended to be more violent in nature with vast humanitarian sufferings.[190] Van Creveld identifies low intensity conflicts by three principal characteristics:

[190] Van Creveld, *The Transformation of War,* 20.

- LIC's unfold in the lesser developed parts of the world except for smaller-scale armed conflicts within developed countries that fall under the label of terrorism.
- LIC's rarely involve regular armies on both sides, but rather regulars on one side and guerillas, terrorists and parts of the population on the other side
- LIC's do not rely primarily on high technology collective weapons usually found in modern forces

Failure to properly recognize these characteristics is perhaps the reason why so many LIC have turned out negatively for modern militaries. The American retreat in the Vietnam War, and similarly, the Soviet defeat in Afghanistan stand out as examples in this regard. The dependency on large maneuver formations and an over reliance on superior technology and weapon systems are part of the explanations for these failures. There is also a tendency to underestimate the political and logistical costs of fighting such wars at a distance even if superior technology and strategic lift capability enable regional or global reach.

Another reasons why Western militaries resist changing their doctrines to include what Van Creveld sees as "the dominant form of war in our age"[191] is the long standing culture of fighting wars according to a "Clausewitzian universe." Arguably, contemporary low-intensity conflicts do not follow a trinitarian paradigm[192] where war is predominantly waged by governments for political ends, but rather a non-trinitarian paradigm where the people, or factions within the people, employ warlike violence to achieve a variety of objectives.[193] In this paradigm, the methods of violence, rules of conduct and the perception of the legitimacy of targets differs vastly from Western ideas about war as they have developed during the last two centuries. Van Creveld's

---

191 Van Creveld, *The Transformation of War* 29

192 Clausewitz' trinity consists of the people, the commander, including his army and the government. Connected to each are dominant tendencies in war. Primarily associated with the people are blind natural forces such as primordial violence, hatred and enmity. To the commander is the play of chance and probability within the limits of his creative abilities. Last is the subordination of war to policies where the political aims are the business of the government alone. Clausewitz, 101.

193 Van Creveld, *The Transformation of War,* 33-62

interpretation of Clausewitz' trinitarian analysis may seem somewhat narrow, [194] but it is incontestable that Western militaries have not been very successful in adjusting their doctrine, organization, training and technological innovation efforts to meet the challenges at the lower end of the conflict scale. As a result, we have difficulties in changing our mindset in the post Cold War environment and continue to resist change; As described in a pertinent remark by General Anthony C. Zinni, USMC (Ret.), on the military culture for changing missions in the nineties, "Traditional military leaders insisted on holding the line to fighting the Nation's wars and hoped to go back to "real soldering" as they were mending a transitioning force suffering from all the pressure on it."[195] Now, in the twenty-firts century it is time to adhere to these missions properly. In a globalized world, former archenemies have joined forces in the GWOT, and it is widely recognized that efforts must be made to solve the problems with the non-integrating part of the world. Principally, this may be done either by exporting security to the most urgent trouble spots, or by establishing sufficient protection against these states' export of terrorism, drugs, criminal activity, or in the worst case WMD. In either case, these strategies must also consider the impact of new technological and sociological trends imposed by the information age.

B. SMART MOBS - THE NEW TECHNOLOGY ENABLED SOCIAL REVOLUTION

Arguably, the information revolution has turned cyberspace and the infosphere into an arena not only for the military, but for terrorists and insurgents as well. Netwar by networked non-state actors has long been emerging as a new threat. The term netwar was first coined by Arquilla and Ronfeldt in 1996, and further developed; "Netwar is the lower-intensity, societal level counterpart to our earlier, most military concept of cyberwar"…"it is composed of conflicts waged, on the one hand, by terrorists, criminals, and ethnonationalist extremists; and by civil-society activists on the other. What

[194] See amongst other Michael Handel *Masters of War* where he compares Sun Tzu and Clausewitz with the presumption that these two historical strategists represent opposing paradigms. His conclusion, however, is "that the basic logic of strategy, like that of political behavior, is universal" (xvii). In addition, studying Clausewitz requires a study of the "Clausewitzian" system as whole and not separate concepts and citations for which Clausewitz is perhaps best known for the typical reader.

[195] Anthony Zinni, "A Military for the 21st Century: Lessons from the RecentPast", *Strategic Forum* No. 181, July 2001. http://www.ndu.edu/inss/strforum/h6.html (accessed 20 April 2004).

distinguishes netwar as a form of conflict is the networked organizational structure of its practitioners - with many groups actually being leaderless - and the suppleness in their ability to come together quickly in swarming attacks."[196] To be fully effective, a netwar actor has to be effective at five levels of theory and practice, "the technological, social, narrative, organizational and doctrinal level."[197]

One of the most recent terms in the netwar arena is Howard Rheingold's concept of smart mobs. Rheingold emphasizes the increased development of wireless and mobile devices and their ubiquitous nature. When these devices get extensively embedded in the population, there is a potential of a new social revolution due to the ways of using them. The affordability and availability of this technology is in fact increasing in most countries. In Norway, for instance, 800 000 new MMS mobile phones are expected to be sold during 2004.[198] Considering Norway's population of only 4.5 million, this new technology will be quickly embedded in the population. MMS stands for Multimedia Messaging Service and these phones have the ability to transmit pictures, animations and sound in addition to text messages. The sociological consequences of this new MMS technology are difficult to predict. One emerging trend is that ordinary people now are acting as "phone journalists,"[199] seeking out events as they occur or have just happened to be at the right place at the right moment. Consequently, ordinary people are currently influencing journalism in a new and exiting manner.

These often unpredictable sociological effects are at the core of Rheingold's smart mob concept. "The people who make up smart mobs cooperate in ways never before possible because they carry devices that possess both communication and computing capabilities."[200] Hence, it is the enhanced potential for cooperation for beneficial or destructive purposes that is revolutionary. The smart mob concept fits within Arquilla and Ronfeldt's notion of netwar but focuses mainly on the social dimension.

---

196 Arquilla and Ronfeldt, *Networks and Netwars,* ix.

197 Ibid.

198 Arve Henriksen, *Telefonfotografene er overalt* Aftenposten, 4 March 2004. http://www.aftenposten.no/nyheter/iriks/article744946.ece (accessed 30 April 2004).

199 Henriksen

200 Rheingold, *Smart mobs – The Next Social Revolution,* xii.

The term smart mobs is difficult to grasp as Rheingold himself admits: "Smart mobs are an unpredictable emergent property that I see surfacing as more people use mobile telephones, more chips communicate with each other, more computers know where they are located, more technology becomes wearable, more people start using these new media to invent new forms of sex, commerce, entertainment communion, and, as always, conflict."[201] With greatest impact to the latter, Rheingold's main points on the potential power of smart mobs can be summarized as follows:

- Ability to form dynamic ad hoc alliances based on many-to-many, real time communication networks (161)
- Ability to swarm and network in a decentralized organized structure (162)
- The massing crowd is not only an effect of technological devices, but the crowd can be seen as a kind of technology itself (160), meaning that the presence or assembly of people/crowds creates the necessary infrastructure, C2 arrangements and means of communication.
- Recognizes and connects like-minded people or people with the same in-plugged interests.
- Forms and distributes both real time and analytical information and creates intelligence networks by websites, peer-to-peer journalism, and text messaging (164-168).
- Ability to form mobile ad hoc social networks where everyone in a smart mob is a "node" with social links (170).
- Ability to form ad hoc mobile information systems that are self-organizing, fully decentralized, and highly dynamic (171).
- Triggers a diversity of cooperation thresholds among individuals that can tip a crowd into a sudden epidemic of cooperation - bandwagon effect (174)
- Inherent capability of collective intelligence where the online social network knows more than the sum of its parts, meaning, for instance, that the network can make collective decisions that are more accurate than the performance of the best individual predictors in the group (179-181)

In short, Rheingold argues that mobile telecommunications enable people to act together in new ways and in situations where collective action was not possible before. Networks, peer-to-peer communication, swarm intelligence, collective knowledge and ad-hoc crowd action are some of the trends that Rheingold foresees might bring about a

[201] Rheingold, 182.

social reorganization on a larger scale. His prediction of social change is not only based on the inherent capability of new technology but more importantly on emerging trends in how people and crowds are, often unintentionally from the manufactures' side, using new technology to organize and interact. Admittedly, it will take a decade, if not more to see profound changes in society and social relations as a whole, but we can already now observe changes in how people meet, mate, work, fight, buy, sell govern and create.[202]

C. REVOLUTIONARY CHANGE

If one accepts the idea that wireless mobile devices will be more common and that the ubiquity of communicating chips will increase, it is natural that social behavior will change, as it has done before with pioneering innovations such as the telegraph, telephone, railroads, automobiles and aircraft. Logically, if social behavior changes, the nature of low-intensity conflicts such as guerilla warfare will change also since basically it is rooted in the population. Guerilla warfare is often referred to as people's war. In broad terms, people's war is any form of popular insurrection or guerilla conflict that has its origin in the internal population, regardless of ideological roots. [203] Whether social behavior in general will change in a revolutionary manner is another question. At least that was not the case with the innovations mentioned above, no matter how important they were for mankind. In this context, the term revolutionary will be reserved for social changes "that involves the intrusion of violence into civil social relations."[204] A sudden or profound change in other aspects of social behavior due to technology or other intervening factors might deserve to be called revolutionary, but in order not to confuse the two, a distinction is needed.

Social change by revolution occurs when other means have failed and the social system is in disequilibrium. Different theories of revolution attempt to explain how this disequilibrium occurs. Commonly, they can be divided in four basics groups:[205] (1) *Actor oriented theories* focus on the personal dimension. The types of individuals or groups that

[202] Ibid, xiii

[203] Gordon.McCormick, "Peoples War" in J. Ciment (ed), *The Encyclopedia of International Conflict* (Shocken Press, 1999), 23.

[204] Chalmers Johnson*, Revolutionary Change,* (Stanford: Stanford University Press, 1982), 1.

[205] Johnson, 170-185

engage in revolutions, their motivation, and how they channel and trigger a situation are common questions in actor oriented theories. (2) *Structural theories* focus on structural components and the social situation including class structure. They see revolutions as normal people's reactions to abnormal situations, independent of cultural influence. They have a long-term historical perspective and the outcome of revolution is important to evaluate and classify the theories. Some of the conditions for revolution are a state's disadvantaged position internationally and internal peasants' revolt, in addition to a distracted elite. (3) *Conjunction theories* combine actor and structural theories in an inclusive context. They emphasize lifecycles, the different stages, social order and distribution of political power. Causes of social movements are explained by the dis-synchronization of social relationships among particular groups. Actor oriented variables are used to explain the attraction to the movement and the influence of leaders' personalities and capabilities. Structural variables assess the likelihood of a movement becoming revolutionary. Political structures and regime toleration towards a movement becomes important. (4) Last are the *process theories* that emphasize contingency; one change will lead to the next and so forth. They realize the complexity of the real world and that pathways are not possible to predict from the outset. They also try to explain, not only the changing strategic vision of the parties during conflict, but also the unintended consequences of the different actions. Both Lenin and Mao realized the need of flexibility and adaptability to changing situations. Consequently they avoided actions and restrictive dogmas until the revolution was secured.

Even if we admit smart mob theory has the potential of profound social reorganization, it cannot explain social revolutionary change within the chosen definition. A social disequilibrium is not likely to be created because of new information technology or collective intelligence in online social networks. Also, with reference to the many ongoing low-intensity conflicts today, it is naïve to believe that smart mobs will end violent rebellion because of a higher state of human cooperation based on democratic values. However, within all the four described revolutionary theories, smart mob theory may enlighten some of the processes that occur in revolutions. Smart mobs have the potential to reinforce some of the processes, increase people's awareness and make things happen more quickly. Understanding smart mob behavior can be particularly useful in

process and actor oriented theories. If recent larger demonstrations are examined, they have a chaotic and anarchistic nature, which makes the outcome of any mass gathering unpredictable. Nobody knows what is coming next or how violent a crowd is going to be. Mass gatherings also have the potential to be manipulated by strong individuals or groups with a more determined purpose. In the longer run, if the profound changes in social behavior that Rheingold predicts turn out to be correct, smart-mob behavior may contribute to structural theories, first and foremost still as enablers for individuals, groups or different classes to express their opinions, and to organize and communicate. Secondly, if we believe in the development of a higher collective intelligence for mainly good purposes, we may see an equalization of knowledge, power and even goods based on smart-mob behavior. However, the former is a more realistic path and it will be characterized by evolutionary and not revolutionary change. The latter will remain as a revolutionary but utopian ideal. In the following this view will be elaborated by looking more specifically at the emergence of insurgencies.

The development of an insurgency, if it is internally and not in response to an occupation, is usually a long and complicated process which can be divided into several phases. The number of phases depends on the levels of analysis. Krepinevich suggests three phases in his account for the South Vietnamese and American defeat in the Vietnam War.[206] *Contention* is the first phase including the insurgent agitation and proselyteization among the masses. Second comes the *equilibrium* phase where the guerillas seek overt violence, guerilla operations, and the establishment of bases. Third is the *counteroffensive* that includes open warfare and overthrow of the existing regime. Certainly, a subsequent phase of *consolidation* always follows a successful insurgency. This phase has been problematic in several revolutions. Different factions within an insurgency may maintain cohesion during the struggle against the incumbents but antagonism often surfaces when the new rulers distribute or retain power and benefits. Often this "revolution within the revolution" has a dividing line between party leadership/intellectuals and peasants/proletariat.[207] However, even if the story doesn't

[206] Andrew Krepinevich Jr, *The Army and Vietnam*, (London: The John Hopkins University Press, 1986), 7.

[207] J. Scott, "Revolution in the Revolution: Peasants and Commissars", Theory and Society, 7 (1979), 130.

end in phase three; the story of the new incumbents starts. The following figure[208] illustrates an insurgency lifecycle throughout its phases:

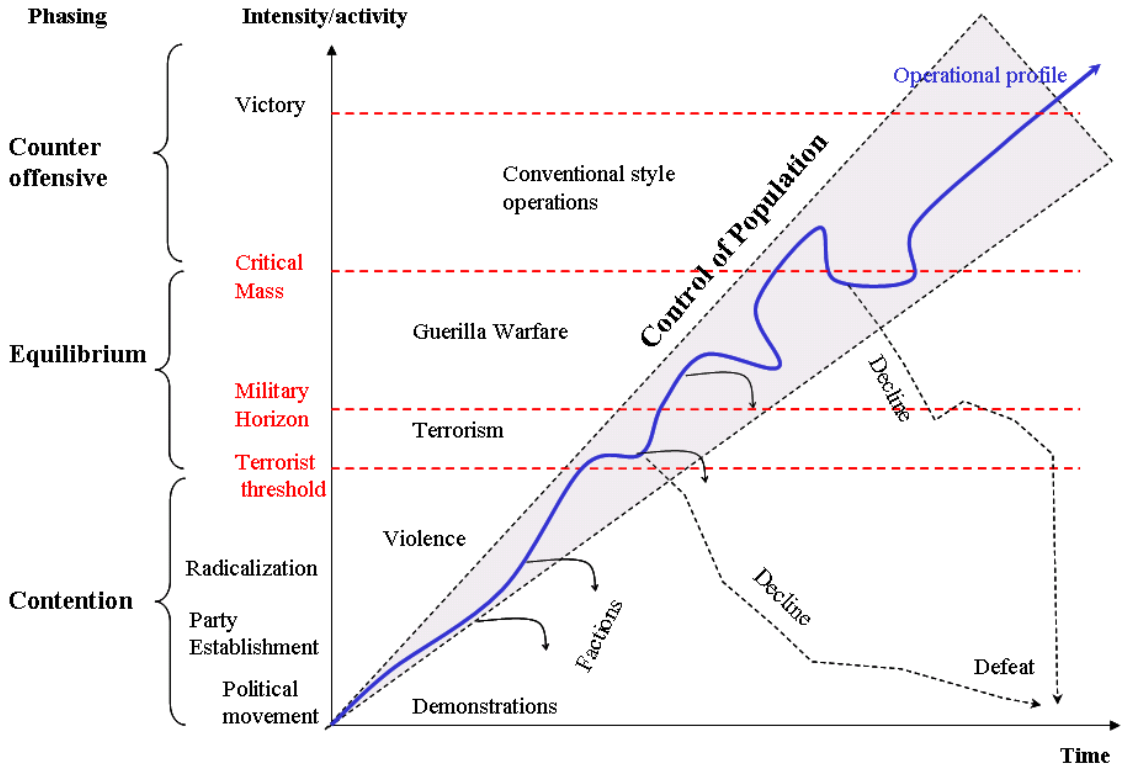

Figure 10. Insurgency Lifecycle (Adapted from McCormick, 2003)

The efficiency of smart mobs depends on how well they support the insurgent strategy. In a pure insurgency, strategies and tactics are centered against three axes, the insurgent - population, the state - population and the insurgent - state axis. To make a difference, smart-mob strategy must support the insurgent's ability to control the population and, over time, muster popular support for its cause. By many scholars this is the far most important axis and from where an insurgency derives its strength. The relationship between the axis and the prioritized insurgent, or counter state strategies are depicted in the upper triangle of the following figure.[209] The lower triangle of the diamond shows the prioritized strategies (not numbered) for a partisan movement. A pure

[208] Adapted and inspired from Gordon H..McCormick, Naval Postgraduate School: Course in Terrorism and Guerilla Warfare 2003.

[209] Adapted from G.McCormick, Naval Postgraduate School, Guerilla Warfare class, summer 2003

partisan movement will depend heavily on support from countries or groups within the international community.

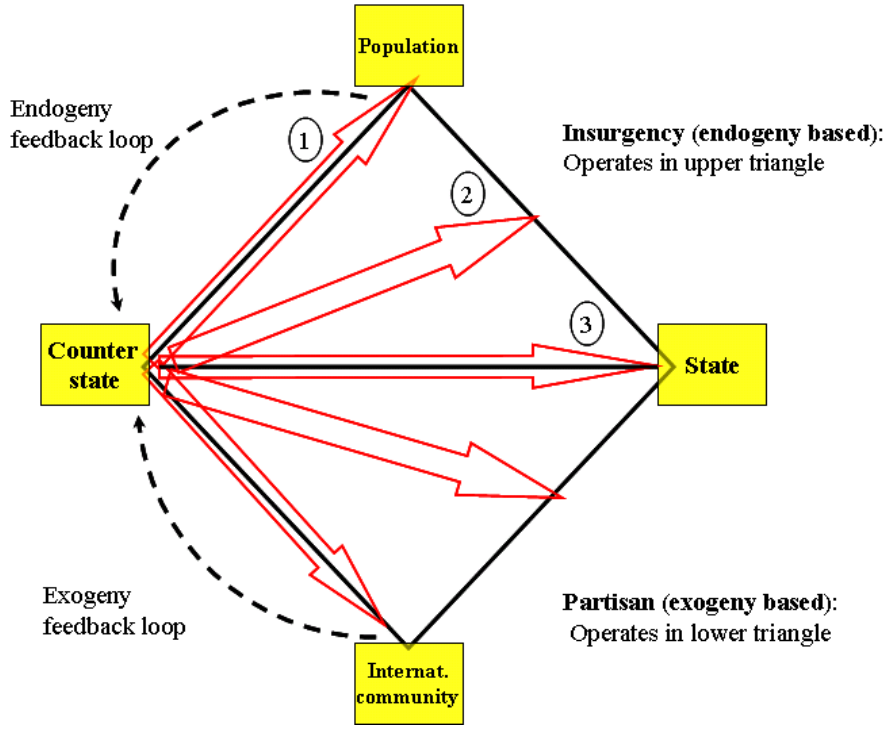

Figure 11. Guerilla Strategies (Adapted from McCormick, 2003)

To achieve victory, whether the guerillas are an insurgency or partisan movement, they eventually have to exercise control over the internal population, either voluntarily or by repression (strategy 1). They are also dependent on support (logistically and politically) from the population. This supply side at work, from either the internal (endogeny) or external (exogeny) environment, is represented by the feedback loop in the Figure. At the same time the insurgency will try to impair the incumbent's relationship with the same population (strategy 2). Of particular interest is how the smart-mob concept may or may not enhance these strategies during the different phases of an insurgency. Less focus will be placed on strategy 3 in this thesis

1. The Contention Phase

The contention phase is perhaps the phase were smart-mob strategies may have the greatest impact. Early in this phase, in an environment not yet characterized by violence, it will be easier to demonstrate, spread propaganda, connect with the like-minded, and form alliances. It is also the phase where people are most likely to "jump on the bandwagon" because the incumbent's tolerances to the movement are expected to be more forgiving and the punishment for opposition less severe. Altogether, smart mobs might even contribute to a "bloodless revolution." This is one of the most optimistic hypotheses on the consequences of smart mobs. Although Rheingold shows both sides of the anticipated social revolution, he emphasizes the positive side, "Technologies and methodologies of cooperation are embryonic today, and the emergence of democratic, convivial, intelligent new social forms depends on how people appropriate, adopt, transform, and reshape the new media once they are out of the hands of engineers - as people always do".[210] Implicit, if humankind is able to reach such a level of higher cooperation, the need of terrorism and armed rebellion will diminish because large portions of the population will have the opportunity to support, oppose or demonstrate their political preferences in a manner and scale never experienced before.

If a revolutionary movement manages to direct the energy of smart mobs efficiently to support its cause, it might demonstrate such an overwhelming opposition that the incumbents see the futility of denying people the desired social change. Moreover, revolutionaries do not actually need to have the majority of the people behind their cause as long as the popular demand is a regime change in general. Power may be conquered anyway in the wake of a regime change if the movement is mature, ruthless or powerful enough, or if its political opponents are sufficiently weak. In a sense, this is what happened in 1917 during the October revolution in Russia. The Kerensky government failed to implement reforms after the Tsar fell in February the same year, and the bourgeoisie and opportunistic labor parties failed to unite their efforts against the advancing Bolsheviks.

The Russian Revolution might be an extreme case of a society in disequilibrium but it shows how a certain movement exploited a chaotic situation. Arguably, also in

[210] Rheingold, 214.

modern times, smart mobs can create these windows of opportunity, which revolutionaries can exploit. As an example of a bloodless revolution in less extreme circumstances, Rheingold points to the Philippine people's spontaneous overthrow of President Estrada in January 2001. Estrada resigned after massive demonstrations. Over a four-day period more than a million people found their way to the streets to demand his resignation. Allegedly, this massing of the crowd was a self-organized ad hoc event as a result of the Philippine population's adaptation to a new mobile and wireless technology; mobile phone texting. According to Rheingold, the Estrada takedown is but one of many early warning signs that we should "…expect the second order effects of mobile telecommunications to bring a social tsunami."[211] Other cases where smart-mob behavior has influenced politics are:[212]

- The "Battle of Seattle" 30 Nov 1999; demonstrators protesting the meeting of the World Trade Organization (WTO) used "swarming tactics", mobile phones, Web sites, laptops and handheld computers to organize and coordinate their efforts.
- British citizens blocking fuel delivery (Sep 2000) in protest against gasoline prices using SMS, e-mail and radios in a wildcat political protest.
- Toronto (spring 2000); violent political demonstrations covered by roving journalists with online webcast digital video.
- San Francisco; since 1992, thousands of bicyclists assemble monthly for "critical mass" moving demonstrations. The critical mass operates through loosely linked networks, alerted by mobile phone and email trees.

Undoubtedly, new information technology and telecommunications are changing the way democratic rights are exercised. However, social change by revolution occurs when other means have failed. The Philippine case stands as an example where mass demonstrations succeeded in overthrowing a regime. History shows other results; in Tiananmen Square, in Beijing in 1989; the Spring demonstrations in Prague 1968; and in several Latin American countries during the last century, peaceful or low violent demonstrations have been quelled by brutal force. What is telling in the Philippine case and in other recent demonstrations is the ease with wich the protesters have mobilized

211 Rheingold, xvii.

212 Ibid, 158

and organized their efforts. The outcome, however, is decided by other factors, as explained in the theories of revolutionary change. For instance, in variables such as the country's democratic tradition and the incumbent regime's tolerance or de facto ability to control their own military and police forces. Also, in Manila, the protesters agreed on the overthrow, but there was no particular political movement or ideology that inspired them. Even if Estrada, due to the ignorance of his corruptive behavior, still had large support in the rural areas, the common identifier was to get rid of him, almost regardless of his successor.

That is not the case with a revolutionary movement, for instance, based on a Marxist-Leninist ideology, as many revolutionary movements have been during the last century. Many of these movements, initiated and led by intellectuals, see the use of violence for social change as a necessity. Hence, a violent strategy is part of their operational profile from the outset. Other groups, such as the peasantry or the working class are useful and needed to create and grow an insurgency; but, as indicated earlier, "…while elites and peasants may come to share a common religious or political identification, their nominal unity disguise sharp contradictions in the meaning, content, and practice of their respective faiths".[213]

Today, a revolutionary movement could ease the process of mobilizing the population using smart-mob strategy and technology. By mobilizing their supporters and manipulating other networks to participate they can muster the masses. The objective is, of course, to put pressure on the incumbents, either to initiate reforms, or to provoke the regime to initiate repressive countermeasures that will attract more supporters. Looking at the violent demonstrations that occur almost everywhere when the world's top leaders gather, be it in the WTO, G7, EU or other types of conferences/summits, one may wonder who is used by whom. A variety of groups or networks appear, from left to right wing extremist, anarchists, environmentalists, students and - just ordinary people. Truly peaceful demonstrators get drawn into violent crowds and increase the impression of a large, angry and determined crowd. Sometimes the effects are devastating. Even in peaceful Sweden, people get shot and killed by the police. In June 2001, over 20, 000

[213] Scott, 102.

people gathered in Gothenburg to demonstrate against president Bush and the EU summit. An aftermath report half a year later summarized it as a weekend of total chaos and fear.[214] The material damage was substantial, hundreds were injured, and the police randomly chased people. Nearly 500 people were temporary imprisoned and a large number were also prosecuted. Later also came the political consequences in forms of harsh criticism against the Swedish government and the police forces. The incident serves as an example of the great potential of manipulation and exploitation of demonstrators where most of them actually had peaceful intentions. Even the successful protest organization, Action pour la Taxation des Transactions pour l'Aide aux Citoyens (Attac), founded 1998 in France and largely involved in organizing the demonstrations in both Seattle (1999) and Gothenburg, claims a non-violent line of action. Despite good intentions, the potential for manipulation is great for those with a more serious intent and, so far, it is the hooligans that get the blame.[215] Hence, smart mobs can be very useful for any revolutionary movement in the early phase of an insurgency.

Besides the noise these demonstrations create in Western democracies, the important lessons learned are about the chaotic and anarchistic nature of modern demonstrations, which make the outcome of any mass gathering uncertain. Equally important is the potential manipulation of these mass gatherings by strong individuals or groups with a determined purpose. Also demonstrated by these cases, and in recent terrorist attacks by organizations like al-Qaeda, is that Rheingold's optimistic view of a higher level of cooperation and collective intelligence for only good purposes seems very naïve and distant at the moment.

The largest obstacle towards such a "convivial and democratic" development, to use Rheingold's own words, is perhaps the nature of smart mobs themselves. The easier to mass crowds, the easier it will be to mass counter forces. The focus of smart mobs will tend to shift in such an environment. Today we see these counter forces at work between the right and left wing movements in Europe. The leftists monitor skinheads, Nazi

---

214 H.Bårdsgård and N.Svensson, "Sjokkrapport om Skandalehelga I Göteborg" *Dagbladet,* 15 Desember 2001. <http://www.dagbladet.no/nyheter/2001/12/15/301333.html> (accessed 18 September 2003).

215 Conclusion in evaluation from the Norwegian Ministry of Justice of the Gothenburg riots (http//www. odin.dep.no/jd/norsk/publ/rapporter/012101-990219/ index-hov004-b-n-a.html)

supporters, and other right winged extremists, and vice versa. Counterdemonstrations are arranged and political meetings are disturbed. Individuals are surveyed, put on public "death lists," harassed and sometimes attacked. Consequently, smart mobs are inherently unpredictable and unstable over time. In a social system that seeks equilibrium they will tend to balance each other more like different *ad hoc interest groups*. In this perspective smart mobs will be just another way of organizing people, and to coordinate and distribute political views. Hence, it can be difficult for a revolutionary movement to take advantage of smart-mob strategies unless the timing and social conditions are advantageous.

2. The Equilibrium Phase

An insurgency cannot remain in the contention phase as an anonymous diverging subgroup in society. Not achieving their goals by "peaceful" means, violence now becomes a significant trademark. The insurgency can either move into a more or less temporary phase of terrorism or it may resort to guerrilla operations directly (see Figure 10). Once the movement has come "out of the closet" it has to maintain momentum, grow and mobilize support for its cause. The Zapatista National Liberation Army (EZLN) in Mexico did so very successfully against the Mexican government in 1994-1998. When open hostilities broke out the guerrillas changed their strategy after only a few days of costly and futile traditional guerrilla tactics and adopted a new form of "social netwar," which by many can be said to represent the world's first "post-modern" insurgency.[216] The most important features of this new strategy[217] were an organizational shift from centralized and battalion-sized formations to decentralized and much smaller maneuverable formations. The second was the insurgents' campaign to mobilize and utilize transnational NGOs and activists to support their cause. A variety of ad hoc networked actors engaged in campaigns, demonstrations, marches and peace caravans against the Mexican regime demanding democracy through nonviolent means; respect for human rights; a cease-fire and withdrawal by the army; peace negotiations; freedom of

216 Arquilla and Ronfeldt, *Networks and Netwars,* 171.

217 Ibid. , 180.

information; and respect for the NGO's role in the conflict.[218] The mobilization for the insurgents' cause strongly constrained the Mexican government's responses and admissions but equally important is the influence it had on the insurgents' goals, which changed from a regime change to democratic reforms. In this sense the Zapatista movement, including the engagement by networked actors, transformed the conflict from a traditional guerrilla insurgency into an information-age social netwar.[219]

Depending on factors such as the ability to mobilize international support, centralized or decentralized leadership, intellectual or peasant dominance of ideas, or the urban or rural origin of the conflict, other revolutionary movements in the information age may not transform and continue to seek an equilibrium based on violent means. In these cases a few interdependent conditions become important if smart-mob strategies are to enhance the insurgent cause. The first condition is the widespread use of smart-mob technology in society in general. To be useful in an internal conflict the technological infrastructure must be comprehensive and smart-mob behavior must be internalized in the population. Otherwise, in spite of smart mob efficiency, the insurgency will stand out as a vulnerable target. They have to have the ability to hide within, or exploit, the normal population's signatures in cyberspace and the infosphere. Hence, smart-mob behavior will be more efficient in technologically sophisticated societies or where wireless technologies such as mobile phone texting is extensively used by the population To use Mao Zedong's terms; guerillas must be like fish in the water - indistinguishable from the indigenous population and its environment. Only then can smart-mob behavior and technology be effective in a true insurgency. The picture is slightly different in a partisan movement. These groups will depend more on the global Internet and long distance communication than wearable communication devices in order to secure support. That is an entirely different circumstance since the hook up nodes can be fewer, the technological infrastructure, including critical nodes and servers, are placed abroad - outside of the incumbent's reach. Also out of reach is the receiver of information or propaganda. Only later, even late in phase 3, do they really need to control the indigenous

[218] Ibid. , 181

[219] Ibid. , 187.

population and, by that time, the partisan movement may have transformed to a classical political and military hierarchic organization.

The second condition is that the technological means that enables smart mobs to function must have a certain level of security. The security of future wireless networks and devices will depend on several factors. An important but very uncertain one, is how the wireless Internet will be regulated in the future. Both merchants, such as hardware, software and Internet providers, and governmental agencies can instigate privacy intrusion but for different purposes. Merchants would like to collect personal information about their users to tailor their products and gain market shares.[220] This may include inbuilt "silent" communication, unnoticeable by the user, between wireless devices when they are online. The result may be a collective self-surveilling population that leaves behind traceable signals. Governments may also want to regulate the use of bandwidth and number of providers by license policy, which will make it easier for them to retrieve information. In addition there are unsolved legal issues on the protection of privacy in cyberspace. Another issue is that every electronic signal that travels in the air may be picked up by electronic countermeasures. Although, new and almost unbreakable encryption codes are available to the public, just the bearing of these signals may be enough to prevent their use.

Another possible development is a free and public innovated mobile Internet with a variety of networks and standards that will be far more difficult to survey. In addition, "experience shows that the information-recording and transmitting equipment used to bolster a regime can be equally handy in subverting it. Devices declared tamper-proof by their manufacturers will nevertheless be tampered with."[221] Such a development combined with the first condition in place, may offer enough freedom of maneuver in the information domain for the insurgents to operate. This freedom of maneuver is a necessity for smart mobs to operate. The greatest difference between smart mobs and other networked actors lies in the fact that the former are mainly technology enabled. In Arquilla and Ronfeldt's terms a networked actor does not necessarily need to be

220 Rheingold, 187.

221 Van Creveld, 211.

technology dependent. They emphasize that "Old technologies, like human couriers, and mixes of old and new systems may do the job in some situations."[222]

Still remaining is the third condition, trust in networks. Not only must security be sufficiently taken care of, but also the social relationships and the information exchanged between networks and individuals must be trusted. Naturally, this is of outmost importance when an individual's life is at stake or when a whole group might be jeopardized. Most likely, the use of cyberspace for malignant purposes will trigger the apparatus of surveillance, enforcement and enactments even in democracies. Intrusion and deception into the insurgencies own network is another source of distrust.

More significantly, the social relevance of trust in modern contemporary societies has also changed throughout the last decades. Pjotr Sztompka has identified some of these changes, which reveal to some degree that the strength of smart mobs is also their weakness in an insurgent environment.[223] Firstly, a smart-mob insurgency is interdependent on other networks in which they cannot exercise absolute control. In addition to the lack of control, these networks consist of a variety of individuals and groups from different social layers that may or may not share the insurgencies' beliefs, values and objectives. The anticipated higher level of cooperation also becomes a source of uncertainty. In Sztompka's words: "Cooperation - of intra-societal as well as inter-societal scope becomes a pressing need, a crucial challenge, but also the domain of uncertainties."[224]

Secondly, technology itself creates uncertainty and unintended consequences that are not compatible with an insurgency of limited resources. An insurgency cannot allow its existence to depend on technology that, as all PC users have experienced, inherently will fail from time to time.

Third, is the complexity of institutions, organizations and technology. In addition to a leadership that may have the intellectual and technological capability to equip and conceptualize wireless mobile devices into smart-mob strategy, the mainstream users are

---

[222] Arquilla and Ronfeldt, *Networks and Netwars,* 11.

[223] Sztompka, *Trust*, 11-13.

[224] Ibid. , 12.

ordinary people. Peasants or working class guerillas may be familiar with mobile phone texting, but if they don't understand the technology behind it, for instance the technological possibility to trace a signal, mistakes will be made that their opponent can exploit.

Fourth is the anonymity and impersonality of the wireless net. In an environment where your very existence depends on your supporting peers and connected networks; personal knowledge or long established relationships of trust seem like a prerequisite. These requirements will largely limit the extension of the insurgency network and consequently also the power of the mobile many.

Last is the inevitable presence of strangers in smart mobs. "To cope with strangers, trust becomes a necessary resource"[225] Due to the perilous nature of an insurgency, the problem is that the guerillas usually have no second chance to recover once the trust has been misused.

If the above conditions are not present to a certain degree, smart-mob insurgencies will certainly experience what J. Bowyer Bell claims to be the inherent inefficiency of the underground. Moreover, Bell highlights the deadly realism of a movement that is forced to operate underground. Revolutionary movements are "inherently inefficient, a price paid for the capacity to persist."[226] If Bell is correct, persistence must be characterized as the minimum level of cooperation, far below the expected dividend of a smart-mob concept. Bell argues that some of the obstacles of operating in the underground are a constant strain - making everyday activity difficult; an inefficient and dysfunctional secrecy policy; difficult command, control and communication arrangements - causing amongst others, a lack of debate and collective decision making and organizational problems.[227] Lastly, but of outmost importance for smart mobs, is that a revolutionary movement needs a liberated zone in which to operate. A zone "where proper authority can be displayed, where the dreams can be seen above

---

[225] Ibid., 14.

[226] J.Bowyer Bell, "Revolutionary Dynamics: The Inherent Inefficiency of the Underground", *Terrorism and Political Violence*, Summer 1990.

[227] Ibid. , 194-203.

ground and at work."[228] The whole idea of smart mobs is the development of a higher level of cooperation and collective intelligence. If the constraints of being in an underground become so heavy, as Bell suggests, the whole foundation of smart mobs will fall apart. A smart mob needs to be extroverted and sociable to influence the population. If this is not achievable, only the hard-core insurgents in their own networked fashion will remain. In this sense smart mobs will be no different from any other netwar actor.

3. The Counteroffensive

The third phase of an insurgency is the counteroffensive that includes open warfare and overthrow of the existing regime. Again, the efficiency of smart-mob behavior will differ whether the guerillas are insurgents or partisans. With part of the organization working abroad, shielded from the local battlefields, the partisans can maintain their activities in the information domain and continue to communicate and influence public opinion, their supporting nations, NGOs or other non-state actors. Smart mobs will usually have more freedom of maneuver to operate internationally depending on their affiliations to terrorist, crime or other shady activity. In contrast, for the insurgency, most of the constraints that were discussed for phase 2 still apply. However there are two differences. Assumable, when operating more conventionally, the insurgents also have established more permanent bases and extended their control over the population in certain areas. If desired, they may more safely resume smart-mob strategies in these or adjacent areas, to further establish trust and influence. On the other hand, the insurgency may not want to see a reemergence of smart mobs. As discussed earlier, smart mobs are unpredictable and inherently allow other networks with other ideas and values to enter. Revolutionary movements are based on some kind of religious, ideological or political ideas. It is questionable that they will allow smart mob interferenced in their own system. Particularly not after a prolonged battle that most certainly has involved human suffering. Hence, the very strategy that helped in an earlier phase now becomes a threat. Besides, being armed and in control, the insurgents now have more suppressive means to gain control if other types of persuasion should fail.

[228] Ibid. , 200.

The other difference is the typical reorganization of the guerillas during phase 3. If the current regime does not give in voluntarily, its power base eventually has to be destroyed by defeating the incumbent's military and police forces. In order to be efficient on the battlefield, the guerillas must reorganize, and they often do so in a hierarchical and conventional manner. In these systems anarchy-like smart-mob behavior has fewer conditions for development. What remains are the strategic or tactical elements of cyberwar or netwar activities. Information technology will still be useful, even crucial to gain victory, but most likely not in a smart mob context.

Lastly, late in phase 3 when the insurgent victory seems likely, it is conceivable that people will jump on the bandwagon to be associated with the winning side. However, this is not true smart-mob behavior, just a natural way of avoiding unpleasant consequences. Still, mass uprisings among the people in the last stages have the potential to shorten the war and lessen casualties significantly.

D. IMPLICATIONS OF SMART MOB STRATEGIES FOR NCW

The implications of smart mob behavior for further developing a NCW concept are many, but two stand out. First and foremost are the requirements of network centric forces to understand and predict the consequences of this type of behavior by opponents or actors in low-intensity conflicts. For instance, mass gatherings are extremely challenging for military forces not trained nor experienced in police-type work. Nevertheless, they will occur wherever military forces are engaged in nontraditional missions. The frequent and violent demonstrations in Kosovo and Iraq have proved to be very difficult for militaries to handle and there is always a danger that they might escalate, turning into very unfavorable events for the forces whose objectives originally were to stabilize and protect. In this sense, the insurgent strategies depicted in Figure 11 apply to the incumbents, but with opposite signs. Hence, understanding the sociological impact of the latest trends in the information age will be important both to counter insurgent, terrorists and extremist strategies and tactics and to avoid or lessen negative reactions in the population of the same. Preemption and prevention based on extensive HUMINT and SIGINT intelligence efforts, can choke a mass uprising before it bursts into flames; but, time is of essence here since these situations may rapidly escalate.

Containment of key individual's or groups' influence on larger crowds, following current police-principles as seen in Europe before and during large sports events, is one efficient method, but it has to be swift and forthright. However, it demands extensive interagency cooperation and legal justification. Another method is to expose ill-intended actors' motives publicly and beforehand. This requires detailed knowledge about the key actors and their modus operandi. The proposed and inherent capabilities of information enabled network centric forces have a better prospect of defeating malicious smart-mob behavior if their design includes nontraditional missions as well. For Norway's case, the armed forces should be well suited to include these capabilities in the doctrinal development of NCW with their long tradition and experiences in military peace keeping and peace enforcing missions.

Another important aspect in the development of new wireless information technologies and smart-mob types of strategies are the possibilities of developing new doctrinal concepts for homeland defense. In Norway's case, an example could be to introduce NCW capabilities in the home guard. The home guard in Norway is a considerably large resource,[229] and one could imagine the impact of such a force if it were truly able to operate autonomously with the advantages of new information technology combined with the force's detailed local knowledge of the cities and rural territories. Moreover, the force is already embedded and integrated in society with multiple civilian and military nodes and network connections. With the proper doctrinal development it could be the key actor in homeland defense alone or in conjunction with domestic and allied reinforcements. Neither should one disqualify the Afghan model from being used in Norway as well in future worst-case scenarios. In such a model the home guard would function as the qualified and required indigenous force.

The reason a *proper* doctrinal development is mentioned is that, although a modernization of the home guard is recognized, the basic features of the force are not likely to change according to the MoD's and Chief of Defense's latest proposal. They

229 "The operational structure of the Home Guard will in future include 50,000 personnel with a further 33,000 in reserve. Personnel will be organized into rapid reaction forces, reinforcement forces and follow-on forces together with a reserve. The number of Home Guard districts is being reduced from 18 to 12, while the system of division into districts, sectors and areas will continue." MoD, Proposition to Parliament No.42 (2003-2004) – Short Version , 2004.

suggest an upgrading and modernization of the equipment in order to solve "important tasks relating to protect infra structure, force protection for national and allied forces and storage facilities."[230] Except for a differentiation in the reaction time for different types of home guard forces, the tasks remain static and nearly the same as they have been throughout the last decades.

Another path could be the NCW approach, taking advantage of the common home guard's every day use of mobility and wireless technologies, which is likely to be carried anyway, and use it for service purposes. The idea of systematically using assets for mobilization purposes in the population is nothing new in Norway. Everything, from cars, buses, motorcycles and even bicycles have been requisitioned. In the information age, laptops, wireless networks, and cell phones could be added to the list. More important, however, is the need to make these units autonomous, but with the ability to interact and operate with other forces entering their area. Or, home guard units could deploy outside their traditional local boundaries, depending on the situation. This requires a higher degree of situation awareness and ability for self-synchronization, which should be possible if the home guard concept is rethought in terms of smart mobs and the characteristics of networked low-intensity actors. Even developments of swarming tactics could be possible, if the different home guard territories and entities are seen in conjunction with each other. However, a NCW approach for the home guard requires a release from a limiting set of static tasks and probably also a deliverance from the conventional army's command and control dominance and doctrinal influence.

E. CONCLUSION

In this chapter the phenomena associated with smart-mob behavior in low-intensity conflicts within a social context has been discussed. Although, smart-mob behavior is based on developments in information technology, particularly in wireless networks and wearable mobile devices, it is the anticipated changes in social behavior that are significant. Other aspects of smart-mob strategies adequately find their place within, for instance, Arquilla and Ronfeldt's netwar and networks concepts. Consequently, all the possible benefits an insurgency may have of the emergence of

[230] MoD, Proposition to Parliament No.42 (2003-2004) – Short Version, 13.

mobile wireless devices for strategic and tactical purposes have not been discussed. These benefits can be substantial, but at the same time severe constraints apply. Emphasis has been on the newest trends of smart-mob behavior centered against the insurgent problem of getting control over the population while depriving the incumbents the same opportunity.

The greatest benefits of smart-mob behavior seem to occur during the first phase of an insurgency. Tolerance within certain regimes may allow smart mobs and transnational networked actors to operate and evolve. This allows the insurgency to display its message, mobilize support for its cause and establish local and global networks and connections. Because of smart mobs anarchistic or uncontrollable nature, large crowds may be manipulated and encouraged to demonstrate. Recent mass gatherings linked to the world's top leaders' summits have more than often turned into violent riots. In societies characterized by social disequilibrium, there is a potential for revolutionary movements to seize power in the wake of a regime change sparked by the mobilization of the masses; but, the timing and social conditions must be advantageous. There are also prospects for smart-mob behavior to increase people's democratic rights by effectively massing the crowds. However, whether the outcome, as in the Philippine case, can be characterized as a "bloodless revolution" depends more on social structures, culture and democratic traditions within society than the convincing power of the mobile many.

As the insurgency moves further up the spiral of violence and eventually crosses the thresholds of terrorism and the military horizon, smart-mob behavior will be risky and less beneficial. Severe constraints, such as the lack of comprehensive wireless networks and mobile devices in the population, security issues and distrust in online social relationships and information, reduce the effects of smart-mob strategies. Furthermore, the realism of an insurgency being in the underground is not easily compatible with the overt activity and needed space of smart-mob behavior. This applies to the information and cognitive domains as well as mass gatherings in the physical space. Eventually, when the insurgency transforms into more hierarchical and conventional style of political and military organizations, smart-mob strategies are no longer required nor wanted. On the

contrary, depending on revolutionary movements' political, ideological or religious standpoints, smart-mob behavior may represent a threat to the new regime.

To conclude, smart mobs and networked actors are likely to change the way democratic rights are expressed and fought for in the future. They may influence social reforms, as seen in the Zapatista movement or even cause regime changes, as in the Philippine case, when certain societal circumstances are in place. However, severe constraints apply to smart-mob strategies in revolutionary movements that have no other choice or seek to reach their goals by violent means. In this conflict category, the information and cognitive domain will also become more important with computerized C2 aid, electronic sensors for more efficient intelligence, and wireless mobile devices that enhance both parties' strategies and tactics. But in the end, it will still be the battles in the physical world that matter. These battles are, as they always have been in internal low-intensity conflicts, characterized by many restraints, brute and cruel violence, and fierce hand-to-hand combat on the ground that will make smart-mob behavior difficult.

The strategic and societal consequences of the information revolution in low-intensity conflicts should also influence how NCW-type forces develop their doctrines and organizations in the future. First and foremost is the ability to understand and predict the consequences of smart-mob type behavior by opponents or other networked actors in order to counter these strategies properly. The vulnerabilities inherently found in smart-mob strategies should be taken advantage of. Detailed knowledge about key actors and their modus operandi is required in this regard. In addition, there are also doctrinal and organizational opportunities in smart-mob strategies that could be exploited to enhance, for instance, a country's concept of homeland defense.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION - TRANSFORMATION IN A NETWORK CENTRIC DIRECTION

A. NETWORK CENTRIC WARFARE AND TRANSFORMATION STRATEGIES

Early in this thesis military transformation was defined as an optimizing strategy that weighs changes in doctrine, organization, capabilities, training, education and logistics in order to fit the defense structure to current and future security challenges. The Norwegian transformation process is explained as a wheel where concept development, doctrine development, operational lessons learned and technological development interact in the transformation process. Interacting links between these elements contribute to an adaptive defense structure.[231] The focus of this thesis has been the strategic factors that are influencing the NCW concept and subsequent doctrinal development.

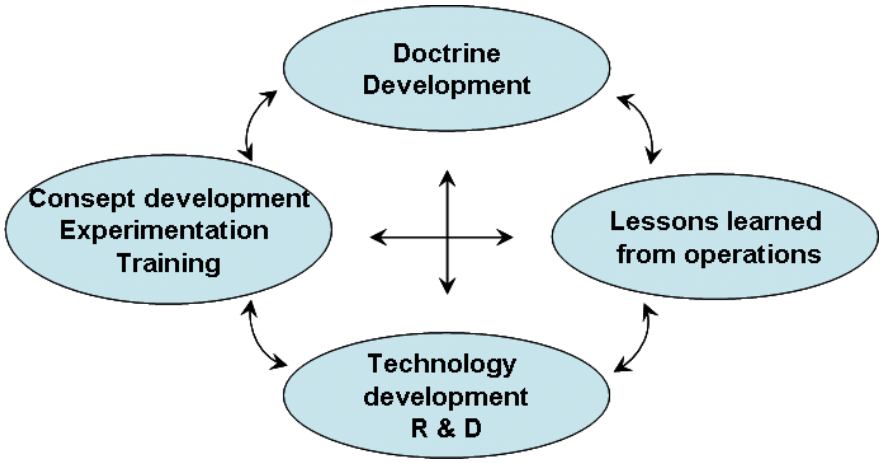

Figure 12. Transformation Wheel (MoD, 2003)

However, the term transformation does not fully describe the underlying vision or the different warfighting concepts that transformation efforts are supposed to support. Clearly, a proactive process that aims to "create a defense organization which is better able to manage unpredictability and the broad spectrum of defense tasks"[232] is an optimal

[231] MoD, Proposition to Parliament No.42 (2003-2004) – Short Version, 5.

[232] Ibid.

goal, but when the transformation process itself gets as much attention as it arguably has at the moment, combined with a wilderness of new terms, fragmented ideas and experimental concepts, it is not easy to identify or understand what the underlying visions or key concepts of the transformation really are. There is a danger that the term will become as unsettling as the term RMA became in the U.S. military in the late nineties as a framework for explaining the emergence of new warfighting concepts. Hence, RMA was replaced by *transformation* by the National Defense Panel to revitalize the innovative processes initiated by, amongst other studies, *Joint Vision* 2010.[233] It is argued that similar concerns still exist and, concerning the Norwegian transformation process, defense policy and military planning for the next long-term period are not yet pointing out any coherent new warfighting concept. The old and official Norwegian defense concept, which also determines the current doctrine developments, [234] remains. This concept is certainly not visionary, but it does state some important values and political guidelines. Four mutually reinforcing principles constitute the defense concept:

- A balanced and flexible national defense.
- Military co-operation with allies and participation in international defense-related co-operation.
- Total defense concept and other civil and military defense-related co-operation.
- The principle of conscription.

Clearly, this concept is not aiming to move the military into the information age and there are no other comprehensive, visionary and authoritatively Joint Future 2020-type documents based on Norwegian conditions that may transform the Norwegian armed forces into netcentric type units for the information age. The significance of not having such a common point of departure is unfortunate because it allows all types of ideas, both antiquated, bureaucratic consolidated, and innovative, to mix in an uncoordinated fashion. A better vision of the future seems to have become the transformation process itself, aiming at an adaptive defense structure where the "Norwegian Armed Forces shall be a learning, vibrant and leading organization - that deliver what is needed, when

[233] William Owens, "The Once and Future Revolution in Military Affairs," *Joint Forces Quarterly*, Summer 2002, 58.

[234] Norwegian Chief of Defense, *Forsvarets Fellesoperative Doktrine Del A - Grunnlag*, Oslo, February 2000, 14.

needed, where needed."[235] Coming, as it does from the MoD, this vision is also authoritative, and certainly, operational concepts and doctrines for the information age will be developed accordingly within the transformation wheel. The question is whether such a vision is specific enough to provide necessary guidelines in a 10 - 30 year perspective, as the function of a vision or defense concept in reality should do to ensure proper doctrinal developments.

The emerging Norwegian approach to NCW has the prospect of becoming a new and authoritative concept with the potential to provide the necessary guidelines, but it needs to be expanded. So far, concept development is operationally and tactically focused, based on networking the different components within the military structure using new information technology. This thesis has offered an analysis of some of the strategic factors that need to be studied if NCW shall become the key defense concept for the information age. Moreover, NCW is part of the transformation process, but not yet at the core as it should be, in order to transform the military from the industrial age into information age forces.[236] The defense minister's New Year speech at the Oslo Military Society exemplifies this. Her speech highlighted eight important challenges:[237]

- Compulsory military service – the cornerstone
- Modernized Officer Candidate Schools
- More junior officers with experience
- Predictable availability of personnel for operations
- From support structure to activity and the "sharp end"
- Quality upgrade for the Home Guard
- A network-based defense
- Strategic management of investments

Although these challenges were not specified in a prioritized order, "a networked -based defense" stands out as an isolated effort. In conjunction with the other issues it

---

[235] MoD, Proposition to Parliament No 42 (short version), 5

[236] Admiral Arthur Cebrowski in Testimony delivered on "Military Transformation" before the Senate Armed Services Committee Hearing. Washington, D.C, 9 April 2002

[237] Kristin Krohn Devold,: *From course change to military transformation* New year address at Oslo Military Society. January 2, 2004. http://odin.dep.no/fd/engelsk/aktuelt/taler/statsraad_a/010011-090093/dok-bn.html (accessed 24 Feb 2004).

signals that NCW is not yet seen as an imperative and integrated part in the transformation process. If it were, the list could in fact be turned upside down, where the other issues were addressed in the context of NCW. In its present form, NCW might not be the proper concept or even right term to use for how Norway should contribute with military means to future conflicts, but we have enough theory, experiences and related experimental doctrines to outline a more tangible and comprehensive concept. In this regard, the Norwegian adapted term *Network-Based Defense* or perhaps *Net-centric Defense* may be more appropriate than the term *Network Centric Warfare,* because it is not specifically war related and includes entities outside the military force structure. It encompasses all levels of conflicts and could also meet the requirements of net-centric activities, cooperation or integration across services, joint units, inter-agencies and multinational entities. Thus, NCW is just one aspect and becomes the warfighting concept, as IW is to IO, used during time of crisis or conflict to achieve or promote specific objectives over specific adversaries. This distinction is more than semantics considering the emotional effect of the term "warfare" to non-military actors, whom net-centric operations very much depend upon.

Furthermore, focus on transformation is good for changing the organizational culture, making units and individuals receptive for change. But too much focus on the process can also be counterproductive. Transformation involves such a broad spectrum of technology, organizations, culture and processes[238] that without direction, it produces opportunities for excuses to do "business as usual," or to display the impressions of urgent activities, within the disguise of clever "buzzwords" that in fact are non-productive. An intense transformation process, aiming to change every aspect of the organization could also be too much to ask for, since the organization itself must create the incentives to transform.[239] In a vaguely defined transformation process this may be extremely difficult because such a process will depend heavily on bottom up engagement in addition to good leadership. Arguably, the emerging NCW concept has much better potential to substantiate and unite the many challenges and objectives currently "floating"

---

238 Admiral Arthur Cebrowski in Testimony delivered on "Military Transformation" before the Senate Armed Services Committee Hearing. Washington, D.C, 9 April 2002

239 Cindy Williams in Michèle Flournoy et al "*What do we mean by "Transformation"* (Naval War College Review, Winter 2002), 32

in existing transformation strategies. Thus, the continuous process of a transformation strategy may continue as a corporate strategy for MoD and defense management, but the process needs tangible direction in addition to just being proactive and flexible. The key point is that without a relatively clear vision of the future, or at least a reasonable achievable concept of why, against whom and how military affairs are going to be conducted, it will be difficult to realize expedient military transformation in the information age and beyond. Consequently, if NCW offers the prospect of delivering what its proponents suggests, it should be at the core of every main objective in the Norwegian transformation efforts.

B. TOWARDS A NETWORKCENTRIC CONCEPT

Highlighting networking as the key strategic and operational concept for the future implies some changes for the transformation strategies that lie ahead. Mentioned earlier was the method of rapid spiral transformation to achieve the desired agility in the transformation process. As a point of departure, some of the issues discussed in this thesis can be viewed within this strategy. The rapid spiral transformation process consists of three parts that must be seen in conjunction with each other.[240] Part one consists of continuous small steps of evolutionary changes; part two features many medium jumps exploring new opportunities; and part three involves taking a few big jumps that could be revolutionary. The key is to fit these three different approaches to a terrain of future strategic, operational and tactical challenges accordingly. The different approaches imply different risks and gains considerations, and each change needs to be studied closely before implementation. However, full knowledge of anticipated consequences will never be achievable, and without taking risks, the dividends can be expected to be equally small. It must also be remembered that even small steps may entail large risks insofar as a military's own competitive advantage is dependent on its opponent's innovative strategies and force capabilities as well.

[240] John Hanley, "Rapid Spiral Transformation" .DoD Office of Force Transformation, *Transformation Trends* – 3 Februar issue 2003. http://www.cdi.org/mrp/transformation-trends.cfm (accessed 26 Feb 2004).

Some of Norway's capabilities connected to homeland defense and the protection of vital interests are areas that ought to be explored in continuous small steps. Without predictable consequences, these capabilities should be sustained and developed in an evolutionary manner, with the objective to keep them on a local maximum. The conscription system and the systems for preserving and defending Norwegian maritime interests are some of the capabilities which should be carefully analyzed with regard to the consequences before major changes are implemented. For instance, the current Coast Guard concept has been developed over decades and has managed to build a well-founded trust among the coastal population, the domestic fleet and international actors in Norwegian waters. The usability of this force may be increased in a military sense by exploiting the force even more with regard to better network centric capabilities and operational concepts, but its primary mission must never be forgotten. On the other hand, many of the network centric capabilities needed for command and control will also enhance the usability of the Coast Guard in its primary role as well. In addition, the likelihood that a crisis could evolve from a minor incident in the North Atlantic is quite possible. An important aspect of the NCW concept is also the ability to understand any situation earlier and in a broader context. Preemption of conflicts is a major goal. This will involve entities used for everyday operations as well as combatant elements. Therefore, units such as the coast guard, maritime patrol aircraft, border patrols, and security forces should be equally netted to the larger and "sharper end" of the network. Similarly, if the compulsory military service system is not adjusted to offer conscripts a meaningful service within a new information age defense structure, it will slowly decline, drawing valuable resources away from a professional force in need of large investments in new materiel and doctrinal development. Consequently, a continuous evaluation of these capabilities must take place and when the time is appropriate larger changes may be introduced. A conscription system that focuses on older and better educated conscripts, instead of today's eighteen to twenty-year olds, can be more useful for NCW forces engaged in, for instance, information intensive low-intensity conflicts. Also, gender may mean less in a net-centric compulsory service, which opens for new discussion on the possibility of drafting women as well as men. Ultimately, before changes are made, these issues must be grounded in dynamic and farsighted NCW doctrines.

In most other areas of the Norwegian defense structure there is a need for many medium jumps that will continuously explore and expand the current capabilities within new doctrines, organizations and technological systems. The benefits of upgrading some of the legacy forces in a "hi-low" mix of entities that will promote doctrinal NCW development have been pointed out. The slogan that "quality counts more than quantity" might be particularly true for information age forces, but old capabilities should not discarded without measuring them thoroughly against a net-centric concept. Technological sophistication does not automatically translate to NCW capabilities and much can be done by simpler means. For instance, local knowledge is better achieved by those who still inhabit the area than by satellite or air surveillance, and runners can still transport vital information as well as the electromagnetic spectrum. Not all information will be time-critical in a NCW concept. Thus, in a Norwegian context, it is extremely valuable that a capability such as the Home Guard, which also involves preserving one of the most important qualities in a country's homeland defense - the will to fight - is continued and seriously integrated in a NCW implementation. In fact, with a proper doctrinal development for the Home Guard, in conjunction with professional forces and allied reinforcement, an overall credible homeland defense could be maintained. That would contribute to resolving one of the main lines of disagreement in the Norwegian transformation process, namely the usability of entities in both an allied and homeland context.

Development of a NCW Home Guard capability may be an example of the larger jumps that also are part of a rapid spiral transformation strategy. Other factors that may change the Norwegian MoD and the defense structure profoundly have also been discussed. An increased use of the elements of soft power is one area where the benefits could be large. Truly exploiting the elements of IO and public diplomacy require a fundamental cultural change in how we collect, process, and distribute/display information, but the end-result could significantly change how we conduct future operations. Together with the different types of knowledge needed to understand friends and enemies in the information age, and in what many believe will be the dominant form of future wars - low-intensity conflicts - the information requirements will fundamentally change the intelligence business, influence concepts of command and control, and

redefine military organizations at most levels. The functions of intelligence: collection, counterintelligence, analysis and covert action,[241] must change and focus more on information that is likely to influence friends', allies' and adversaries' information and cognitive domains more than their physical capabilities. This is nothing new in military affairs, since influencing decision makers has been a crucial aspect since the days of Sun Tzu. However, the information revolution enables processing and analyzing more complex information structures than a single commander's brain ever could, which can be difficult enough, considering the unpredictability of recent adversaries such as Milosevic and Hussein. Moreover, the information revolution coupled with a reorganization of intelligence efforts may enable the understanding and prediction of complex concepts such as smart-mob behavior and tipping points. Taking into consideration these latest sociological trends in the information age can prove to be decisive if information age forces are to fight "smarter" in the future. Few have doubts about the RMA hypothesis on the conventional battlefield and for high-intensity armored warfare, but this is not the form of war where Western countries will meet their greatest challenges in the future. [242] Even if Norway is geographically located at a "safe" distance from most of the world's trouble spots, this type of exported security is expressively stated as a mission for the Norwegian military. Consequently, doctrine development and the incorporation of relevant NCW capabilities that enable the armed forces to operate in an LIC environment will be increasingly more important in the future.

In conclusion, and as depicted in the model for strategic planning which was the starting point for this thesis, the impact of NCW development has been set in a strategic perspective. The aim was to identify some of the factors that are important to understanding subsequent mission challenges, opportunities and constraints. In most areas, NCW concepts entail so many profound changes that only a few issues that will have an important impact on future forms of war have been discussed. The underlying premises found in Norway's strategic environment will always be important and should function as a driver in the concept development. Hence, a comprehensive national

[241] Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (New York: The Free Press, 1992), 4

[242] O'Hanlon,

strategy based on Norway's geopolitical situation and vital interest, which also includes a military doctrine, becomes important. Currently, the situation demands a need for comprehensive and independent NCW capabilities in addition to a strong allied affiliation. Likewise, a continuous adaptation of the NCW concept to the features of future potential adversaries and the changing characteristics of the nature of conflict must be emphasized. Many other challenges are barely mentioned. For instance, there are the challenges connected with the NCW implementation process itself. Allied and inter-governmental interoperability, joint force training requirements, the linkage of strategic, operational and tactical levels, and further research and developments, are all issues that will be crucial if the NCW concept is to be realized. Last but not least, the direction of the transformation process itself will be crucial. Vice Admiral Cebrowski stated that, "When we think about transformation we divide it into three distinct areas. Transformation of the role of defense in society; transformation of the management of defense; and force transformation."[243] This distinction is useful to concentrate efforts in a transformation strategy, but one of the main conclusions that emerges from analyzing NCW through strategic lenses, is the fact that the elements of NCW will intervene in all these areas simultaneously - as a truly embedded network should. Consequently, if net-centric operations are seen as the cornerstone in future warfighting concepts, it should indeed be pursued on a broader level in a comprehensive Norwegian transformation strategy. Despite its size, Norway possesses both the resources and competence to do so. It is first and foremost a question of networking national resources. In so doing *Network Centric Defense* has the potential to become a feasible and holistically defense alternative.

[243] Cebrowski 22 January 2003 in speech to the NCW 2003 conference, *Transformation trends* – 17 February issue.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Alberts, David and Richard Hayes. *Power to the Edge.* CCRP Publication Series, June 2003.

Alberts, David, John Garstka, Frederick Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority.* CCRP Publication Series, 1999.

Arquilla, John and David Ronfeldt, *Swarming & The Future of Conflict.* Santa Monica: Rand, 2000.

Arquilla, John and David Ronfeldt. "Swarming: The Next Face of Battle". *Aviation Week & Space Technology,* September 29, 2003.

Arquilla, John, and David Ronfeldt. *Networks and Netwars.* Santa Monica: RAND, 2001.

Bårdsgård, H and N. Svensson,. "Sjokkrapport om Skandalehelga I Göteborg," *Dagbladet,* 15 Desember 2001. http://www.dagbladet.no/nyheter/2001/12/15/301333.html (accessed 18 September 2003).

Barnett, Thomas P.M. "The Seven Deadly Sins of Network-Centric Warfare," *Proceedings*, U.S. Naval Institute, January 1999.

Bass, Carla. "Building Castles on Sand." Air War College: *Maxwell Paper,* No.15, 1998.

Bell, J.Bowyer. "Revolutionary Dynamics: The Inherent Inefficiency of the Underground," *Terrorism and Political Violence*, Summer 1990.

Berggrav, Jørgen. "Militær Transformasjon, en nødvendighet for å møte fremtiden?" *The Norwegian Atlantic Committee, Kortinfo – 3 2003,* August 2003. http://www.atlanterhavskomiteen.no/publikasjoner/andre/kortinfo/2003/3-2003.htm . (accessed 26 January 2004).

Biddle, Stephen. "Afghanistan and the Future of Warfare: Implications for Army and Defense Policy." U.S. Army War College, Strategic Studies Institute, November 2002.

Carey, John et al. "Point, Click…Fire," *BusinessWeek online*, April 7, 2003. http://www.businessweek.com/index.html (accessed 6 March 2004)

Clarke, Wesley. *Waging Modern War.* New York: PublicAffairs, 2001.

Clausewitz, Carl von. *On War.* New York: Everyman's Library Knopf, 1993.

Codevilla, Angelo. *Informing Statecraft: Intelligence for a New Century.* New York: The Free Press, 1992.

Cohen, Eliot. "A Revolution in Warfare," *Foreign Affairs*, Volume 75, no.2, (March/April 1996).

Creed, Douglas and Raymond Miles. "Trust in Organizations: A Conceptual Framework Linking Organizational Forms, Managerial Philosophies, and the Opportunity Costs of Controls." In *Trust in Organizations: Frontiers of Theory and Research,* Roderick Kramer and Tom Tyler,ed. Thousand Oaks: SAGE publications, 1996.

Denning, Dorothy E. *Information Warfare and Security.* ACM Press Books, 1999.

Department of Defense Report to Congress. "Network Centric Warfare." 27 July 2001. www.c3i.osd.mil/NCW/ (accessed 14 April 2004).

Devold, Kristin Krohn. "From Course Change to Military Transformation". New Year address at Oslo Military Society. January 2, 2004. http://odin.dep.no/fd/engelsk/aktuelt/taler/statsraad_a/010011-090093/dok-bn.html (accessed 24 Feb 2004).

Evans, David. "Vincennes ". http://www.odu.edu/webroot/orgs/ao/mo/nrotc.nsf/files/Vincennes.PDF/$FILE/Vincennes.PDF (accessed 24 April 2004).

Gaffney, Frank Jr. "The Tipping Point." *Washington Times*, 16 Dec 2003. http://nl.newsbank.com/nl-search/we/Archives?p_action=list&p_topdoc=11 (accessed 22 April 2004).

Garstka, John. "Network Centric Warfare: An Overview of Emerging Theory." *PHALANX Online,* December 2000 Volume 33 Number 4. Joint Staff Directorate for C4 Systems, ND. http://www.mors.org/publications/phalanx/dec00/feature.htm (accessed3 April 2003).

Giambastiani, Edmund P. "What is Transformation?" *Allied Command Transformation web page*. http://www.act.nato.int/transformation/transformation.html (accessed 12 May 2004).

Gladwell, Malcolm. *The Tipping Point.* Boston: Little, Brown and Company, 2002.

Hammer, Helle. "The Norwegian Shipping Industry". Norwegian Ministry of Foreign Affairs. http://odin.dep.no/odin/engelsk/norway/economy/032001-990368/index-dok000-b-n-a.html (accessed 21 March 2004).

Handel, Michael. *Masters of War*. London: Frank Cass Publishers, 2001.

Hanley, John. "Rapid Spiral Transformation" .Department of Defense Office of Force Transformation, *Transformation Trends.* 3 Februar 2003. http://www.cdi.org/mrp/transformation-trends.cfm Retrieved 26 Feb 2004. (accessed 26 February 2004)

Hayes, Albert. *Information Age Transformation: Getting to a 21st Century Military.* CCRP Publication Series, June 2002.

Headquarters Department of the Army. Field Manual. No 3-0 (FM 3-0), "Operations," 14 June 2001.

Headquarters Department of the Army. Joint Publication 3-13. *Joint Doctrine for Information Operations.* 1998.

Henriksen, Arve. "Telefonfotografene er overalt". *Aftenposten*, 4 March 2004. http://www.aftenposten.no/nyheter/iriks/article744946.ece Retrieved 30 April 2004. (accessed 30 April 2004).

Hundley, Richard O. "Past Revolutions, Future Transformations." Santa Monica: Rand, 1999.

Johnson, Chalmers. *Revolutionary Change.* Stanford: Stanford University Press,1982

Joint C4ISR Decision Support Center: Conference Proceedings, 13-14 January 2003. *Swarming: Network Enabled C4ISR*. http://www.iwar.org.uk/rma/ (accessed 28 April 2004).

Joint Chiefs of Staff. *Joint Vision 2020.* Washington: U.S. Government Printing Office, June 2000.

Kagan, Robert. *Of Paradise and Power*. New York: Alfred A. Knopf, 2003.

Knutsen, Bjørn Olav, Alf Granviken, Mats Ruge Holte, Anders Kjølberg, Finn Aagaard. "Europeisk sikkerhet i en foranderlig tid: En analyse av Norges utenriks- og sikkerhetspolitiske handlingsrom," *The Norwegian Atlantic Committee, Det sikkerhetspolitiske bibliotek nr 4 – 2000,* http://www.atlanterhavskomiteen.no/publikasjoner/sp/2000/4-2000.htm (accessed 26 March 2004).

Komer, Robert. W. *The Malayan Emergency in Retrospect: Organization of A Successful Counterinsurgency Effort.*Santa Monica: Rand R-957-ARPA, February 1972.

Krepinevich, Andrew Jr. *The Army and Vietnam*. Baltimore: The John Hopkins University Press, 1986.

Krohn Devold, Kristin. "Usability through Transformation." Speech at the Norwegian Atlantic Committee's "Leangkollen" Conference. February 2, 2004. http://odin.dep.no/fd/engelsk/aktuelt/taler/statsraad_a/010001-990096/index-dok000-b-n-a.html. (accessed 25 February 2004).

Kuehl, Dan. "Information Operations: The Hard Reality of Soft Power." (not dated). Joint Forces Staff College. http://www.jfsc.ndu.edu/schools_programs/jciws/iw/io_textbook.pdf (accessed 18 May 2004).

Kuehl, Dan. Interview with Wanja Eric Naef about Information Operations, London, July 2003. *Infocon Magazine* Issue One, October 2003. http://www.iwar.org.uk/infocon/print/io-kuehl.htm (accessed 22 March 2004).

Lansford, Tom. *All for One: Terrorism, NATO and the United States*. Burlington: Ashgate, 2002.

Leonard, Mark and Andrew Small. "Norwegian Public Diplomacy." The Foreign Policy Centre, June 2003. Norwegian Ministry of Foreign Affairs http://odin.dep.no/archive/udvedlegg/01/06/ml10_018.pdf (accessed 22 March 2004).

Leonard, Robert. *The Principles of War for the Information Age.* New York: Ballantine Books, 1998.

Leonhard, Mark. *Public Diplomacy.* London: The Foreign Policy Centre, 2002.

Liddell Hart, Basil H. *Strategy.* London: Meridian, 1991.

Lord, Carnes. "The Past and Future of Public Diplomacy." *Orbis 42 (1),*1998.

Lord, Carnes. *Political Warfare and Psychological Operations.* Washington: National Defense University Press, 1989.

Mandelbaum, Michael. *The Dawn of Peace in Europe.* New York: The Twentieth Century Fund Press, 1996.

McCormick, Gordon. "Peoples War." *The Encyclopedia of International Conflict.*. J. Ciment (ed) Shocken Press, 1999.

McEvily, Bill, Vincenzo Perrone, Akbar Zaheer. "Trust as an Organizing Principle." *Organization Science*, Vol.14, No 1, January-February 2003.

Milward, Brinton and Jörg Raab, "Dark Networks: The Structure, Operation, and Performance of International Drug, Terror, and Arms Trafficking Networks." Paper presented at the International Conference on the Empirical Study of Governance, Management, and Performance. Barcelona, Spain, 4-5 October 2002.

Murray, Williamson and Thomas O'Leary. "Military Transformation and Legacy Forces" *Joint Forces Quarterly*, Spring 2002.

NATO. "Prague Summit Declaration." http://www.nato.int/docu/pr/2002/p02-127e.htm. (accessed 25 Feb 2004).

NATO. "The Alliance's Strategic Concept." North Atlantic Council in Washington D.C. on 23 and 24 April 1999. http://www.nato.int/docu/pr/1999/p99-065e.htm (accessed 17 September 2003)

Neumann, Iver and Kristine Offerdal. "Russia is Back." *The Norwegian Atlantic Committee, Internet text nr 18, November 2003.* http://www.atlanterhavskomiteen.no/publikasjoner/andre/i-tekster/18.htm (accessed 24 March 2004).

Neumann, Iver. "Norges handlingsrom og behovet for en overgripende sikkerhetspolitisk strategi". *The Norwegian Atlantic Committee, Kort-info fra DNAK 1-2001* http://www.atlanterhavskomiteen.no/publikasjoner/andre/kortinfo/2001/1-2001.htm Retrieved 26 March 2004 (accessed 24 March 2004).

New, William. "Army Relying on New Battlefield Network Technology." Government *Executive Magazine*, Daily Briefing, 8 April 2003.

Norwegian Chief of Defence. "Konsept for nettverksbasert anvendelse av militærmakt." *Forsvarssjefens Militærfaglige Utredning 2003.* Oslo, 2003.

Norwegian Chief of Defence. *Forsvarssjefens Militærfaglige Utredning 2003.* Oslo, 8 Desember 2003.

Norwegian Chief of Defense. Forsvarets Fellesoperative Doktrine Del A – Grunnlag. Oslo, February 2000.

Norwegian Defense Staff College, "Introduksjon til Nettverksbasert Forsvar," *Militærteoretisk skriftserie* - nr 1 2001.

Norwegian Ministry of Defence. *Norwegian Defence 2004*. Online fact book on Norwegian defense. http://odin.dep.no/fd/engelsk/publ/veiledninger/010011-120064/index-dok000-b-n-a.html. (accessed 5 March 2004).

Norwegian Ministry of Defence. "Defence budget". http://www.dep.no/fd/norsk/publ/veiledninger/010011-120053/index-dok000-b-n-a.html . (accessed 19 February 2004).

Norwegian Ministry of Defence. "The Further Modernization of the Norwegian Armed Forces 2005-2008." Proposition to Parliament No. 42 (2003-2004) Short Version.

Nyhamar, Tore. "Norske Nasjonale Interesser i Nord-Atlanteren," The Norwegian Atlantic Committee *Internet text nr. 11- 2003*. http://www.atlanterhavskomiteen.no/publikasjoner/andre/i-tekster/11.htm (accessed 16 March 2004).

O'Hanlon, Michael. *Technological Change and the Future of Warfare*. Washington DC: Brookings Institution Press, 2000.

Osgood, Robert E. *Limited War: The Challenge to American Strategy*. Chicago: The University of Chicago Press, 1957

Owens, Bill. *Lifting the Fog of War.* New York: Farrar, Straus and Giroux, 2002.

Owens, William. "The Once and Future Revolution in Military Affairs." *Joint Forces Quarterly*, Summer 2002.

Perrow, Charles. *Complex Organizations: A Critical Essay*. New York: McCraw-Hill, 1993.

Potts, David (ed). *The Big Issue: Command and Combat in The Information Age.* CCRP Information Age Transformation Series, February 2003. Reprint from Strategic and Combat Studies Institute Occasional Paper Number 45, March 2002.

Rheingold, Howard. *Smart Mobs: The Next Social Revolution.* Cambridge: Perseus Publishing, 2003.

Shawcross, William. *Allies: The U.S., Britain, Europe and the War in Iraq.* New York: Public Affairs, 2004.

Solstrand, Ragnar. “Teknologi, Forsvar og Forsvarsstrukturer.”Norwegian Defense Institute, 2000, Report 2000/03429.

Swidey, Neil. “Tipping Points: How Military Occupations Sour,” *Boston Globe*, 27April, 2003.

Sztompka, Piotr. *Trust: A Sociological Theory.* Cambridge: Cambridge University Press, 1999.

Thomas, Timothy. “Kosovo and the Current Myth of Information Superiority.” *Parameters*, Spring 2000.

Trustees of Dartmouth College. “Cyber Attacks During the War on Terrorism: A Predictive Analysis.” Dartmouth College: Institute for Security Technology Studies, 22 September 2001.

Van Creveld, Martin. *The Transformation of War*. New York: The Free Press, 1991.

Vego, Milan. “Net-Centric Is Not Decisive.” *Proceedings*, January 2003.

Wentz, Larry. *Lessons from Kosovo.* CCRP Publication Series, July 2002.

Williams, Cindy in Michèle Flournoy et al “What Do We Mean by ‘Transformation’.*” Naval War College Review*, Winter 2002.

Zinni, Anthony. “A Military for the 21st Century: Lessons from the Recent Past.” *Strategic Forum* No. 181, July 2001. http://www.ndu.edu/inss/strforum/h6.html (accessed 20 April 2004).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. John Arquilla
   Naval Postgraduate School
   Monterey, California

4. Gordon H. McCormick
   Naval Postgraduate School
   Monterey, California

5. Dorothy E. Denning
   Naval Postgraduate School
   Monterey, California

6. Jennifer Duncan
   Naval Postgraduate School
   Monterey, California

7. The Royal Norwegian Ministry of Defence
   Oslo, Norway

8. Norwegian Defence Staff College
   Oslo, Norway

9. Defence Staff Norway,
   Chief of the Naval Staff
   Oslo, Norway

10. Norwegian Naval Education and Training
    Bergen, Norway

11. Norwegian Defence Research Establishment
    Kjeller, Norway

12. Norwegian Battle Lab & Experimentation
    Bodo Main Air Station, Norway

13. Marinejegerkommandoen
Ramsund, Norway

14. Hans Liwång
Department of Military Technology
Swedish National Defence College
Stockholm, Sweden